

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-123496

(43)Date of publication of application : 26.04.2002

(51)Int.Cl.	G06F 15/00
	G06F 13/00
	H04L 9/08
	H04N 5/44
	H04N 7/16
	H04N 7/167

(21)Application number : 2000-316395 (71)Applicant : SONY CORP

(22)Date of filing : 17.10.2000 (72)Inventor : EZAKI TADASHI

(54) DEVICE AND METHOD FOR RECEIVING CONTENTS STORAGE MEDIUM AND SERVER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents receiver corresponding to a plurality of RMPs(Right Management and; Protection) systems drawn up in each contents distribution system.

SOLUTION: Only formats for regulating the specifications of the RMPs composed of information such as contents charging security and copyright protection are unified. Each contents provider inputs enciphered contents and right processing information in a format conforming to the unified specification. A contents user side can decode and utilize contents regardless of their PMP system on the same contents receiver only by preparing a plurality of functions corresponding to the respective RMP systems.

CLAIMS

[Claim(s)]

[Claim 1] It is content reception equipment which receives contents distributed in conformity with prescribed right management and protection (Right Management & Protection:RMP) system. A content reception means to receive contents distributing and an identification device which identifies right management and a

protection system of receiving contentsContent reception equipment providing a right processing means which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said identification device.

[Claim 2]Right management and a protection system A cipher system of contentsdistribution systems of a keya contents decryption systemA transmission system of accounting information or keysarchive-medium control informationa system of mutual recognitionAPS (Analog Protection System: a macro visionCGMS (Copy Generation Management System)etc.)The content reception equipment according to claim 1 specifying an indispensable item to content purchase and contents use of viewing limit information etc.

[Claim 3]The content reception equipment according to claim 1 characterized by what it has two or more kinds of right management and protection modulesaid right processing means chooses corresponding right management and protection module based on a discriminated result by said identification deviceand right processing of receiving contents is performed for.

[Claim 4]Have right management and a protection module acquisition means which acquires right management and a protection module from the exteriorand said right processing meansThe content reception equipment according to claim 1 characterized by what right processing of receiving contents is performed for using right management and a protection module acquired from the exterior via said right management and protection module acquisition means based on a discriminated result by said identification device.

[Claim 5]Have right management and a protection module generation means to generate right management and a protection module automatically according to specification description of right management and a protection systemand said right processing meansThe content reception equipment according to claim 1 characterized by what right processing of receiving contents is performed for using right management and a protection module generated by said right management and protection module generation means.

[Claim 6]The content reception equipment according to claim 1 including a contents storage means which accumulates contents.

[Claim 7]The content reception equipment according to claim 1 characterized by what contents before right processing by said right processing means are stored in said contents storage means for including a contents storage means which accumulates contents.

[Claim 8]The content reception equipment according to claim 1 characterized by what contents after right processing by said right processing means are stored in said contents storage means for including a contents storage means which accumulates contents.

[Claim 9]Said content reception meansincluding further a contents storage means

which receives contents distributed in form enciphered with a predetermined key and accumulates contents said right processing means The content reception equipment according to claim 1 characterized by what enciphered content which received is decrypted and is stored in a contents storage means after re-enciphering with other keys.

[Claim 10] Contents distributed in form that said content reception means was enciphered with a predetermined key And including further a contents storage means which receives an enciphering key which enciphered this key and accumulates contents said right processing means The content reception equipment according to claim 1 characterized by what a received enciphering key is decrypted and is stored in a contents storage means with enciphered content after re-enciphering with other keys.

[Claim 11] The content reception equipment according to claim 1 wherein said right processing means accumulates a log of right processing of receiving contents.

[Claim 12] The content reception equipment according to claim 1 characterized by what said right processing means carries out APS (Analog Protection System) processing and does for the external output of the regenerative signal of contents after right processing according to specification description of applicable right management and protection system.

[Claim 13] The content reception equipment according to claim 1 wherein said right processing means enciphers and carries out the external output of the contents after right processing.

[Claim 14] It is a contents receiving method which receives contents distributed in conformity with prescribed right management and protection (Right Management & Protection: RMP) system A content reception step which receives contents distributing and a discernment step which identifies right management and a protection system of receiving contents A contents receiving method providing a right processing step which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said discernment step.

[Claim 15] Right management and a protection system A cipher system of contents distribution systems of a key contents decryption system A transmission system of accounting information or key archive-medium control information a system of mutual recognition APS (Analog Protection System: a macro vision CGMS (Copy Generation Management System) etc.) The contents receiving method according to claim 14 specifying an indispensable item to content purchase and contents use of viewing limit information etc.

[Claim 16] The contents receiving method according to claim 14 characterized by what it has two or more kinds of right management and protection modules corresponding right management and protection module are chosen in said right processing step based on a discriminated result by said discernment step and right processing of

receiving contents is performed for.

[Claim 17]Based on a discriminated result by said discernment step it has further right management and a protection module acquisition step which acquires applicable right management and protection module from the exteriorThe contents receiving method according to claim 14 characterized by what right processing of receiving contents is performed for in said right processing step using right management and a protection module acquired from the exterior by said right management and protection module acquisition step.

[Claim 18]Have further right management and a protection module generation step which generates right management and a protection module automatically according to specification description of right management and a protection systemand in said right processing step. The contents receiving method according to claim 14 characterized by what right processing of receiving contents is performed for using right management and a protection module generated by said right management and protection module generation step.

[Claim 19]The contents receiving method according to claim 14 containing a contents storage step which accumulates contents which received.

[Claim 20]The contents receiving method according to claim 14 containing a contents storage step which stores contents before right processing by said right processing step.

[Claim 21]The contents receiving method according to claim 14 containing a contents storage step which stores contents after right processing by said right processing step.

[Claim 22]Contents distributed in form enciphered with a predetermined key at said content reception step are receivedThe contents receiving method according to claim 14 characterized by what it has for a contents storage step stored after re-enciphering receiving contents decrypted in said right processing step with other keys.

[Claim 23]Contents distributed in said content reception step in form enciphered with a predetermined keyAnd the contents receiving method according to claim 14 characterized by what an enciphering key which enciphered this key is received and it has for a contents storage step stored with enciphered content after re-enciphering a key decrypted in said right processing step with other keys.

[Claim 24]The contents receiving method according to claim 14 provided with a log accumulation step which accumulates a log of right processing of receiving contents in said right processing step.

[Claim 25]A regenerative signal of contents after right processing by said right processing stepThe contents receiving method according to claim 14 characterized by what APS (Analog Protection System) processing is carried out according to specification description of applicable right management and protection systemand it has an external output step which carries out an external output for.

[Claim 26]The contents receiving method according to claim 14 characterized by what

it has for an external output step which enciphers and carries out the external output of the contents after right processing by said right processing step.

[Claim 27]. Are characterized by comprising the following. So that reception of contents distributed in conformity with prescribed right management and protection (Right Management & Protection:RMP) system may be performed on computer systems. A storage which stored described computer software physically in computer-readable form.

A content reception step to which said computer software receives contents distributing.

A discernment step which identifies right management and a protection system of receiving contents and a right processing step which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said discernment step.

[Claim 28] A server comprising:

A means to accumulate two or more right management and protection modules corresponding to each right management and protection system.

A means to answer a demand having contained identification information of right management and a protection system and to transmit applicable right management and protection module.

[Claim 29] A server comprising:

A means to accumulate two or more right management and protection modules corresponding to each right management and protection system.

A means to answer an inquiry based on identification information and to change contents using applicable right management and protection module.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the content reception equipment and the contents receiving method which receive the contents distributed via a broadcast wave or a network etc. It is related with the content reception equipment and the contents receiving method with which a specific user receives the pay content distributed in the form that a movie, music etc. were enciphered especially.

[0002] As for this invention, contents work and providing agents such as a movie and music start the content reception equipment and the contents receiving method to receive in detail for the enciphered content distributed via brokers such as a

broadcasting organization and an Internet Service Provider and it especially is related with the content reception equipment and the contents receiving method with which contents work and the providing agent itself receive the contents which distribute fee collection security etc. about contents use with a controllable form.

[0003]

[Description of the Prior Art] It is increasingly dealt with on information machines and equipments such as a computer with innovation of the information technology of these days as contents by which various medias such as an image and music were digitized. These contents can be distributed by development of information and communication technology using broadcast of a satellite, a terrestrial wave etc. or a broad-based network like the Internet.

[0004] Distribution of an image content or a music content is already carried out partly. According to contents distribution technology a conventional commercial distribution course and physical medium are omissible. Even if it is the consumers of a remote place desired image and music title can be obtained easily. Contents work volition leads also to development of increase and the whole industry by making higher profits with the position by the side of contents work and a providing agent by quick and efficient contents selling. [0005] For example the server type and accumulation type broadcasting system on condition of the TV receiver containing the mass hard disk drive Profits are certainly securable by enciphering and distributing contents such as a movie in the contents distribution contractor of a broadcasting station or others and charging the key for decryption to a contents purchaser i.e. a televiewer at the time of distribution.

[0006] Such a content reception form is also called a CAS (Conditional Access System (limited reception)) system. In drawing 14 the general-view composition of the contents distribution system of a CAS base is illustrated.

[0007] The content provider who makes or provides contents for distributions such as an image and music in the contents distribution system shown in the figure 1 comprises a contents distribution entrepreneur who distributes to consumers the contents which a content provider provides via a broadcast wave or a network and the consumers i.e. three persons of a general user who receive contents.

[0008] The broadcasting organization for whom the contents distribution entrepreneur used broadcasting satellites such as BS (Broadcasting Satellite: broadcasting satellite) CS (Communication Satellite: communications satellite) for example it comprises an Internet Service Provider etc. which manage the broadcasting organization using a terrestrial wave or the connection service to the Internet and the variety-of-information contents providing service on the Internet.

[0009] The general user is installing the content reception machine which receives contents distributing for example in a house. A TV receiver like STB (Set Top Box) may be sufficient as the content reception machine which receives the contents through a broadcast wave for example. A common computer system like a personal

computer (PC) may be sufficient as the content reception machine which receives contents via the Internet for example. A content reception machine contains a hard disk drive and it is preferred that it is a receiver corresponding to the accumulated type broadcast which can accumulate a long time, e.g. an image and a lot of music contents.

[0010] In order for a content reception machine to receive contents via a broadcast wave it is necessary to equip the CAS (limited reception) card corresponding for every broadcasting organization. In order to receive contents via the Internet while acquiring a user account (user qualification) from a predetermined Internet Service Provider beforehand it is necessary to carry out an Internet connectivity via a nearby access point at the time of content purchase.

[0011] What is necessary is just to use the time of CAS card (or receiver which contained CAS) purchase for example in order for a broadcasting organization to collect the expenses and profits which contents distribution takes. What is necessary is just to add the contents fee amount equivalent to the fee paid every month for example in order for an Internet Service Provider to collect the expenses and profits which contents distribution takes. However the charging system by the CAS system or a user account aims to let a contents distribution entrepreneur control the fee collection to each consumer, i.e. contents user.

There is nothing under a content provider's control.

In other words even if a content provider uses CAS of the contents distribution entrepreneur body etc. he cannot secure his profits.

[0012] In order for a content provider to collect a contents fee from general consumers it is mentioned that the content provider itself decides upon contents provision systems (referred to as RMP (Right Management & Protection) below) such as a contents fee security and copyright protection. In RMP more specifically the system of encryption, the distribution systems of a key, a contents decryption system, the transmission system of accounting information or key archive-medium control information, the system of mutual recognition. The indispensable item is included in the content purchase and contents use of APSs (Analog Protection System: a macro vision CGMS (Copy Generation Management System) etc.), viewing limit information etc. In the user and consumer side of contents by preparing the content reception machine which mounted the RMP module corresponding to a content provider, the contents distributing which uses a content provider as a supply source can be purchased on the success reverse side and it can use namely view and listen to it. It may be made to leave the batch management of accounting information to the settlement-of-accounts organization besides a content provider like a control center.

[0013] However the actual condition is deciding upon the RMP system about a contents fee security and copyright protection variously generally for every contents distribution system which each content provider provides. If a contents distribution system is different even if it is the same music content distribution and movie

contents distribution under the environment where two or more systems are intermingled -- the same contents receiver top -- if -- that is [it cannot decrypt] it falls into the situation where contents cannot be used.

[0014] For example if a contents user is going to purchase contents two or more content providers i.e. distribution system The hardware or software of a content reception machine must be prepared for every distribution system it is inconvenient to a user or excessive expenses are needed. As a conclusion with the troublesome content purchase method when a user's contents refrainment from buying arises the profits of contents offer / distribution enterprise will make little increase and the whole enterprise may become calm.

[0015]

[Problem to be solved by the invention] The purpose of this invention is to provide the outstanding content reception equipment and contents receiving method with which a specific user can receive suitably the pay content distributed in the form that a movie music etc. were enciphered.

[0016]. The further purpose of this invention can receive suitably the enciphered content which contents work and providing agent such as a movie and music distribute via brokers such as a broadcasting organization and an Internet Service Provider. It is in providing outstanding content reception equipment and contents receiving method.

[0017] The further purpose of this invention is for contents work and the providing agent itself to provide the outstanding content reception equipment and contents receiving method which can receive suitably the contents which distribute fee collection security etc. about contents use with a controllable form.

[0018] The further purpose of this invention is to provide outstanding content reception equipment and a contents receiving method which can respond to two or more RMP (Right Management & Protection) systems upon which it is decided for every contents distribution system.

[0019]

[Means for Solving the Problem and its Function] This invention is made in consideration of an aforementioned problem and the 1st side effect is content reception equipment which receives contents distributed in conformity with prescribed right management and protection (Right Management & Protection: RMP) system. A content reception means to receive contents distributing and an identification device which identifies right management and a protection system of receiving contents. It is content reception equipment providing a right processing means which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said identification device.

[0020] Work / offer entrepreneur of contents distributes contents in form that encryption etc. were protected according to right management and a protection system called RMP. Generally various right management and protection system are

adopted for every contents work / offer entrepreneur.

[0021] Only by unifying only a form which specifies specification of right management and a protection system according to content reception equipment concerning the 1st side of this invention. An identification device can identify right management and a protection system of receiving contents and the right processing means can carry out right processing of the receiving contents using selectively right management and a protection system applicable based on this discriminated result.

[0022] Therefore only by preparing beforehand a function corresponding to each right management and protection system even if it is a case where contents in accordance with which right management and protection system are received it can respond to several different contents distribution systems using one set of a content reception machine. It becomes unnecessary that it is to be able to decrypt contents on the same contents receiver to be able to appropriate for the use and to prepare apparatus such as a receiver for every distribution system.

[0023] Among each contents work and offer / distribution entrepreneur argument involving standardization of contents distribution systems such as RMP specification description can be calmed down. Compatibility and flexibility of contents distributing between each contents work and offer / distribution entrepreneur can be raised. Convenience increases in a contents user.

[0024] Here right management and a protection system to say A cipher system of contents distribution systems of a key A contents decryption system a transmission system of accounting information or keys archive-medium control information A system of mutual recognition APS (Analog Protection System: a macro vision CGMS (Copy Generation Management System) etc.) An indispensable item is specified to content purchase and contents use of viewing limit information etc.

[0025] Content reception equipment may be beforehand provided with two or more kinds of right management and protection modules. In such a case said right processing means can choose corresponding right management and protection module based on a discriminated result by said identification device and can perform right processing of receiving contents.

[0026] Or content reception equipment may be provided with right management and a protection module acquisition means which acquires right management and a protection module from the exterior. In such a case said right processing means can perform right processing of receiving contents using right management and a protection module acquired from the exterior via said right management and protection module acquisition means based on a discriminated result by said identification device.

[0027] Or content reception equipment may be provided with right management and a protection module generation means to generate right management and a protection module automatically according to specification description of right management and a protection system. In such a case said right processing means can be done

[performing right processing of receiving contents using right management and a protection module generated by said right management and protection module generation meansor].

[0028]Content reception equipment may include a contents storage means which accumulates contents. For examplecontents before right processing by said right processing means and after right processing are storable in said contents storage means.

[0029]Contents which said content reception means receives are enciphered with a predetermined keyfor example. In such a casesaid right processing means decrypts enciphered content which receivedand after re-enciphering with other keysit may be made to store it in a contents storage means. By such compositioncontents after right processing can be protected further.

[0030]Contents which said content reception means receives also receive an enciphering key which enciphered this key further while being distributed in form enciphered with a predetermined keyfor example. In such a casesaid right processing means decrypts a received enciphering keyand after re-enciphering with other keysit may be made to store it in a contents storage means with enciphered content. By such compositioncontents after right processing can be protected further.

[0031]It may be made for said right processing means to accumulate a log of right processing of receiving contents. In such a casea settlement-of-accounts organization can perform exact accounting byfor exampletransmitting an accumulated log to a predetermined settlement-of-accounts organization periodically or irregularly.

[0032]Said right processing means carries out APS (Analog Protection System) processing according to specification description of applicable right management and protection systemand may be made to carry out the external output of the regenerative signal of contents after right processing. In such a casea video recovery signal after right processingetc. can be protected.

[0033]Said right processing means enciphers contents after right processingand may be made to carry out an external output. In such a casea case where contents are transmitted to other information machines and equipmentfor example by a home network course like IEEE 1394Contents can be protected even if it is a case where transmit contents to a computer system like a personal computer (PC) via LANand it processes using application.

[0034]The 2nd side of this invention is a contents receiving method which receives contents distributed in conformity with prescribed right management and protection (Right Management &Protection:RMP) systemA content reception step which receives contents distributingand a discernment step which identifies right management and a protection system of receiving contentsIt is a contents receiving method providing a right processing step which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said discernment step.

[0035]Only by unifying only a form which specifies specification of right management and a protection system according to the contents receiving method concerning the 2nd side of this inventionA discernment step can identify right management and a protection system of receiving contentsand can carry out right processing of the receiving contents in a right processing stepusing selectively right management and a protection system applicable based on this discriminated result.

[0036]In said right processing stepbased on a discriminated result by said discernment stepcorresponding right management and protection module are chosenand it may be made to perform right processing of receiving contents.

[0037]Or based on a discriminated result by said discernment stepit may have further right management and a protection module acquisition step which acquires applicable right management and protection module from the exterior. In such a casein said right processing stepright processing of receiving contents can be performed using right management and a protection module acquired from the exterior by said right management and protection module acquisition step.

[0038]Or it may have further right management and a protection module generation step which generates right management and a protection module automatically according to specification description of right management and a protection system. In such a casein said right processing stepright processing of receiving contents can be performed using right management and a protection module generated by said right management and protection module generation step.

[0039]A contents storage step which accumulates contents which received may be included. For exampleit may be made to store contents before right processing by said right processing stepand after right processing.

[0040]At said content reception stepwhen receiving contents distributed in form enciphered with a predetermined keyit may have a contents storage step stored after re-enciphering receiving contents decrypted in said right processing step with other keys.

[0041]Contents distributed in said content reception step in form enciphered with a predetermined keyAnd after re-enciphering a key decrypted in said right processing step with other keysit may be made to have a contents storage step stored with enciphered contentwhen receiving an enciphering key which enciphered this key.

[0042]It may have a log accumulation step which accumulates a log of right processing of receiving contents in said right processing step. In such a casea settlement-of-accounts organization can perform exact accounting byfor exampletransmitting an accumulated log to a predetermined settlement-of-accounts organization periodically or irregularly.

[0043]It may have an external output step which carries out APS (Analog Protection System) processingand carries out the external output of the regenerative signal of contents after right processing by said right processing step according to specification description of applicable right management and protection system.

[0044]It may have an external output step which enciphers and carries out the external output of the contents after right processing by said right processing step.

[0045]The 3rd side of this inventionSo that reception of contents distributed in conformity with prescribed right management and protection (Right Management &Protection:RMP) system may be performed on computer systems. In computer-readable formare described computer software the storage stored physicallyand said computer softwareA content reception step which receives contents distributingand a discernment step which identifies right management and a protection system of receiving contentsIt is a storage providing a right processing step which carries out right processing of the receiving contents according to applicable right management and protection system based on a discriminated result by said discernment step.

[0046]A storage concerning the 3rd side of this invention is a medium which provides computer software physically in a computer-readable form to computer systems of flexibility which can execute various program codesfor example. Attachment and detachment of CD (Compact Disc)FD (Floppy Disc)MO (Magneto-Optical disc)etc.etc. are free for such a mediumand it is a storage of portabilityfor example. Or it is also technically possible to provide specific computer systems with computer software in computer-readable form via transmission mediasuch as a network (a network does not ask distinction of radio and a cable)etc.

[0047]Such a storage defines a collaboration relation on structure of computer software and a storage for realizing a function of predetermined computer softwareor a function on computer systems. By installing predetermined computer software in computer systems via a storage concerning the 3rd side of this inventionif it puts in another wayOn computer systemsa collaboration operation is demonstrated and the same operation effect as content reception equipment and a contents receiving method concerning each 1st [of this invention] and 2nd sides can be obtained.

[0048]A means by which the 4th side of this invention accumulates two or more right management and protection modules corresponding to each right management and protection systemIt is a server provided with a means to answer a demand having contained identification information of right management and a protection systemand to transmit applicable right management and protection module.

[0049]A means by which the 5th side of this invention accumulates two or more right management and protection modules corresponding to each right management and protection systemIt is a server possessing a means to answer an inquiry based on identification information and to change contents using applicable right management and protection module.

[0050]The purpose,the featureand an advantage of further others of this invention will become clear [rather than] by detailed explanation based on an embodiment and Drawings to attach of this invention mentioned later.

[0051]

[Mode for carrying out the invention]An embodiment of this invention described below

explains content reception equipment which can respond to two or more RMP(s) upon which it is decided for every contents distribution system.

[0052]RMP is the abbreviation for Right Management & Protection and is a concept used by TV Anytime Forum, becoming a problem in a contents distribution enterprise through broadcast or a network — an illegal use of contents — merely seeing and merely hearing it — it is . If this kind of malfeasance overruns contents work and offer / distribution entrepreneur's just profits will not be guaranteed but it will be concerned also with enterprise fate. In other words use right management of contents and protection are required and RMP bears this.

[0053]In RMP more specifically A system of encryption distribution systems of a key a contents decryption system A transmission system of accounting information or key archive-medium control information a system of mutual recognition An indispensable item is included in content purchase and contents use of APSs (Analog Protection System: a macro vision CGMS (Copy Generation Management System) etc.) viewing limit information etc.

[0054]Only a form which specifies specification of RMP which consists of these items is unified and each contents offer entrepreneur should just input enciphered content and right processing information into contents in form in accordance with this specification. In such a case in the side consumers i.e. a contents user who receive and use contents. Even if it is the contents based on what kind of RMP system by preparing two or more functions corresponding to each RMP system it can decrypt on the same contents receiver and can appropriate for the use.

[0055]RMP specification description can be described as a part of metadata which accompanies contents distributing for example. Below a portion relevant to RMP specification description will be called "right processing metadata" among metadata. For example in the case of digital broadcasting etc. metadata can be distributed as data for data broadcasting which accompanies a volume on program book.

[0056]Conceptual composition of a RMP module is shown in drawing 1. A RMP module is built in and used for a content reception machine of a form of STB (Set Top Box) or others and can be mounted using a module of predetermined hardware or software for example. As shown in the figure a RMP module has composition provided with some interfaces for outputting and inputting data about receiving contents.

[0057]The contents downloaded via network such as contents received via broadcast of a satellite wave or a terrestrial wave or the Internet are stored in mass storage devices such as a hard disk drive with metadata. A RMP module inputs receiving contents in the state before right processing directly without passing a hard disk drive course or a hard disk drive.

[0058]Encryption is given to contents bodies such as an image and music for the purpose of contents protection. Therefore the decipherment function (Decryptor) for solving enciphered content is required and a RMP module has an interface for an enciphered content input which inputs enciphered content by the specified

cryptographic algorithm.

[0059] Although metadata is distributed corresponding to each content in the information which shows the right processing and the required right protection about contents, e.g. right processing metadata is included.

[0060] The copy control information etc. of the keys for solving contents, the terms of purchase of contents, a service condition and the decoded contents are included in right processing metadata. A RMP module has an input interface of right processing metadata which inputs the information about right processing or protection according to a regular format.

[0061] Contents distributing is enciphered, for example by a contents key, and this contents key is transmitted with enciphered content with a form further enciphered with a distribution key (Distribution Key). In a RMP module, a distribution key is held, a contents key enciphered using this distribution key can be decoded, and enciphered content can be further decoded using a decoded contents key. While being able to perform contents distribution safely according to such encryption and a transmission system, changing a contents key for every contents by a RMP module, enciphered content can be decoded by holding a single distribution key and it can be appropriate for the use. It may be made for a right processing metadata input interface of a RMP module to input an enciphered content key as right processing metadata.

[0062] Specification about fee collection for contents use upon which it decides in contents work / offer entrepreneur is also included in right processing metadata, and it may be made for a right processing metadata input interface of a RMP module to input this.

[0063] As specification about fee collection, price information, service conditions (reproduction fee collection in every time, number-of-times restrictions which specified the refreshable number of times before, and time limitation made refreshable till the predetermined date, etc.) etc. can be specified, for example.

[0064] For the accounting to a contents user, settlement-of-accounts organizations other than a contents work and offer / distribution entrepreneur like a control center may be established. It connects with such a control center and a RMP module has an accounting interface for performing the transaction about fee collection or settlement of accounts. Whenever it, for example, reproduces the contents accumulated on the hard disk drive, a fee collection log is generated, and it connects with a control center for every prescribed period, and a RMP module transmits a log. On the other hand, the control center can perform fee collection and settling processing based on the log sent by each contents user.

[0065] It is as having already stated to have the interface for enciphered content for a RMP module to input the receiving contents before right processing. A RMP module for the interface for accumulating the contents after right processing in a hard disk drive again for the use covering several times of contents, and permanent / semipermanent preservation of contents, it has the interface for storing the contents

after right processing on removable media such as DVD (Digital Versatile Disc). The interface for the contents storage and reproduction after such right processing can specify existence of an authentication method etc. of the control to media such as encryption of the contents for accumulation and a decoding at the time of reproduction and the attestation to media.

[0066] A RMP module is provided with an external output interface for reproducing receiving contents or contents read from a hard disk drive or a removable media with a display or other external instruments. In an example shown in drawing 1 it has an analog output interface for carrying out a display output on a display as a video signal and a digital output interface for transmitting contents to an external instrument via home network such as IEEE 1394. An analog output interface adopts APS (Analog Protection System) etc. for contents protection of analog format. A macro vision CGMS (Copy Generation Management System) - ASCMS which embed copy control information at a predetermined scanning line of a vertical blanking interval etc. are contained in APS. Attestation bus encryption like 1394CP besides transmitting contents encryption etc. are controllable by a digital output interface.

[0067] Contents after right processing can be transmitted and processing using desired application can be performed on an information management system like a personal computer (PC). A RMP module is provided with the host / interface for applications for outputting contents to an external information management system in an example shown in drawing 1. A host / interface for applications controls encryption of transmitting contents etc.

[0068] Mounting with hardware components for exclusive use can also realize a RMP module also by executing a predetermined program code on a general-purpose processor. Along with contents distributing distribution and distribution of specification about RMP can be done as right processing metadata (above-mentioned).

[0069] An example of a RMP specification description format is shown below.

[0070]

[Mathematical formula 1]

[0071] In the RMP specification description format shown above, the identification information (RMP ID) for identifying the system of RMP is included in the beginning and also, the encryption algorithm which enciphers contents distributing the encryption algorithm which enciphers the contents key K_s used for encryption of contents distributing. The format for accumulating the authentication algorithm and log which are used for the storage key K_{st} used when accumulating the encryption algorithm and contents distributing which encipher the distribution key K_d used at the time of contents distribution and mutual recognition etc. can be specified. Generally as a cipher system DES (Data Encryption Standard) Multi2 etc. are used.

[0072] It is decided upon the specification description as RMP for every contents work

/ offer entrepreneur. Since RMP was conventionally fixed and used for every contents distribution system in order to receive offers of contents from two or more systems excessive expenses such as preparing a new content reception machine were required. On the other hand by specifying the interface for inputting into the specification description of RMP and RMP by this invention it can respond to security systems such as a contents fee in two or more contents distribution systems and encryption and a copyright protection system on the same contents receiver by the RMP module which decoded the specification or suited the specification coming to hand.

[0073] As one real original form of this invention by a content reception machine or the contents recording reproduction inside of a plane. Two or more hardware RMP modules which mounted different RMP specification are prepared and changing and using for a hardware RMP module which suits for every receiving contents is mentioned.

[0074] A RMP module is constituted as a software module as other real original form of voice. Downloading a software module which suits for every receiving contents from a predetermined server or analyzing right processing metadata and generating a desired software module automatically by a content reception machine side are mentioned.

[0075] Two or more hardware RMP modules which mounted different RMP specification are prepared for drawing 2 and composition of the content reception machine 10 of form changed and used for a hardware RMP module which suits for every receiving contents is illustrated typically.

[0076] The content reception machine 10 shown in the figure The front end section 11 and the CAS treating part 12. It comprises the hard disk drive 13A for contents storage and 13B, the RMP identification part 14 and the two RMP modules (plurality) 1 and the RMP module 2 based on RMP specification description different respectively.

[0077] The front end section 11 performs tuning of the broadcast wave of a predetermined channel, i.e. channel selection processing and recovery processing of received data.

[0078] The CAS treating part 12 cancels the scramble processing applied to broadcast contents based on the contract about CAS (Conditional Access System (limited reception)) exchanged among contents distribution entrepreneurs (descrambling). In the digital broadcasting in Japan BS and CS adopt the scrambling system called common "MULT2." However since the CAS processing itself does not relate to the summary of this invention it is not explained any more here.

[0079] The hard disk drives 13A and 13B are used for accumulation of receiving contents. One hard disk drive 13A is used for accumulation of the contents of the state before the right processing by a RMP module and more specifically the hard disk drive 13B of another side is used for accumulation of the contents of the state after right processing. However the hard disk drives 13A and 13B may be the separate storage areas (partition) which do not need to be isolated systems mutually for

example were physically assigned on the single hard disk.

[0080] In this example the peculiar identification information (RMP ID) for identifying the system is assigned to RMP described as a part of right processing metadata. The RMP identification part 14 enables operation of the direction corresponding to RMP ID which read right processing metadata from the hard disk drive 13. Identified RMP ID and was identified among the two RMP modules (plurality) 1 and the RMP module 2. [0081] The RMP module 1 and the RMP module 2 are provided with some interfaces (above-mentioned) for processing the right processing metadata which accompanies contents such as an enciphered movie and music and contents. The RMP module 1 or the RMP module 2 energized by the RMP identification part 14. It operates as the RMP specification description described as right processing metadata and contents processing of a decoding of enciphered content, the external output as reproduction contents, the hard disk drive 13 storing in a removable media etc. etc. is performed.

[0082] To drawing 3 the composition of the content reception machine 20 concerning other embodiments is illustrated typically. The content reception machine 20 prepares two or more hardware RMP modules which mounted different RMP specification is changed to the hardware RMP module which suits for every receiving contents and is used.

[0083] In an example shown in the figure the content reception machine 20 has the front end section 21, the hard disk drive 23, the RMP identification part 24, each RMP module 1 and the RMP module 2, and composition by which interconnection was carried out via the data bus 26 with the same decoder output equipment 25.

[0084] The front end section 21 performs tuning of a broadcast wave of a predetermined channel, i.e. channel selection processing and recovery processing of received data. However, although not illustrated, when receiving contents from a predetermined service provider via wide area networks such as the Internet to instead of [which does not pass a broadcast wave] a Network Interface Card can realize the front end section 21.

[0085] The hard disk drive 23 is used in order to accumulate contents of a state before right processing by a RMP module or to accumulate contents of a state after right processing.

[0086] The peculiar identification information RMP ID for identifying the system is assigned to RMP described as right processing metadata. The RMP identification part 24 enables operation of a thing corresponding to RMP ID which read right processing metadata from the hard disk drive 23. Identified RMP ID and was identified among the two RMP modules (plurality) 1 and the RMP module 2.

[0087] The RMP module 1 and the RMP module 2 are provided with some interfaces (above-mentioned) for processing right processing metadata which accompanies contents such as an enciphered movie and music and contents. The RMP module 1 or the RMP module 2 energized by the RMP identification part 24. It operates as RMP specification description described as right processing metadata and contents

processing of a decoding of enciphered content an external output as reproduction contents the hard disk drive 23 storing in a removable media etc. etc. is performed. When receiving contents from a contents distribution entrepreneur who adopts a CAS system it may be made to carry a CAS module which performs corresponding decryption and descrambling processing on a RMP module.

[0088] The decoder output equipment 25 performs decoding and an external output of reproduction contents after right processing. For example if it is AV content the decoder output equipment 25 will carry out Separation Sub-Division of the contents to a compression video data and compression audio data. And about compression audio data while carrying out the expansion process of the compression video data based on MPEG 2 etc. and reproducing the original video signal after carrying out PCM (Pulse Code Modulation) decoding it compounds with an additional sound and is considered as a reproduced sound signal.

[0089] To drawing 4 composition of the content reception machine 30 concerning other embodiments is illustrated typically. The content reception machine 30 constitutes a RMP module as a software module and downloads a software module which suits for every receiving contents from a predetermined server.

[0090] As shown in the figure the content reception machine 30 The front end section 31 and CPU (Central Processing Unit) 32 The network interface 37 serves as the hard disk drives 33A and 33B the RMP identification part 34 the operation memory 35 and the decoder output equipment 36 with composition by which interconnection was carried out via the system bus 38.

[0091] The front end section 31 performs tuning of a broadcast wave of a predetermined channel i.e. channel selection processing and recovery processing of received data.

[0092] The network interface 37 It is equipment for connecting the content reception machine 37 to wide area networks such as the Internet according to predetermined communications protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol). A countless host terminal is connected on the Internet. Some host terminals are the information distribution servers which distribute contents such as a movie and music and other parts are servers which distribute a software RMP module. When receiving contents from a predetermined service provider via wide area networks such as the Internet instead of receiving contents via broadcast the network interface 37 can realize the front end section 31.

[0093] Under control of an operating system (OS) CPU 32 is a central controller which controls operation in the content reception machine 30 in generalization and executes various kinds of program codes using the operation memory 35.

[0094] The hard disk drive 33A is used for accumulation of contents in a state before right processing by a RMP module and accumulation of contents of a state after right processing. The hard disk drive 33B is used for accumulation of a software (or it downloaded beforehand) RMP module used before. The hard disk drives 33A and 33B

do not need to be isolated—system units respectively for example may be the storage areas (for example partition) divided on a single hard disk drive.

[0095] The peculiar identification information RMP ID for identifying the system is assigned to RMP described as right processing metadata. Right processing metadata is read from the hard disk drive 33. RMP ID is identified and an applicable software RMP module is loaded on the operation memory 35 and the RMP identification part 34 detects whether it is under [present use]. *****. The RMP identification part 34 can also be mounted as a program code which CPU 32 executes as hardware components.

[0096] When a software RMP module on the operation memory 35 does not hit to RMP ID about contents to be reproduced from now on, it looks for an applicable software RMP module on the local disk 33B and this is replaced with a thing on the operation memory 35 when found. When a software RMP module applicable on the local disk 33B is not able to be discovered further, a server on a network can be accessed by network interface 37, of course, and it can look for a desired software RMP module.

[0097] CPU 32, by performing a software RMP module loaded on the operation memory 35, it can operate as RMP specification description described as right processing metadata and contents processing of a decoding of enciphered content, an external output as reproduction contents, the hard disk drive 33A storing in a removable media, etc., can be performed. What is necessary is just to load similarly a CAS module which performs corresponding decryption and descrambling processing on the operation memory 35 in receiving contents from a contents distribution entrepreneur who adopts a CAS system.

[0098] The decoder output equipment 36 performs decoding and the external output of the reproduction contents after right processing. For example, if it is AV content, the decoder output equipment 36 will carry out Separation Sub-Division of the contents to a compression video data and compression audio data. And while carrying out the expansion process of the compression video data based on MPEG 2, etc., and reproducing the original video signal after carrying out PCM (Pulse Code Modulation) decoding about compression audio data, it compounds with an additional sound and is considered as a reproduced sound signal.

[0099] In the form of the flow chart, the procedure for downloading a software RMP module to the content reception machine 30 is shown in drawing 5. Hereafter, the download processing of a software module is explained according to this flow chart.

[0100] When starting reproduction of the contents accumulated in the hard disk drive 33A, corresponding right processing metadata is similarly read from the hard disk drive 33A and RMP ID of a RMP module is acquired (Step S1). And this RMP ID confirms whether it is in agreement with it of the RMP module loaded to the present operation memory 35 (Step S2).

[0101] When the RMP module of the contents which RMP ID hits, namely reproduces after this is already loaded on the operation memory 35, then after carrying out

connection establishment to a control center and performing accounting about content purchase based on RMP specification description (Step S3) contents playback is performed (step S4) and this whole manipulation routine is ended.

[0102] On the other hand when RMP ID does not hit RMP acquisition place information is acquired (Step S5) it connects with the server used as a RMP acquisition place (Step S6) and an applicable software RMP module is downloaded from this server (Step S7). And the downloaded software RMP module is installed in the content reception machine 30 (Step S8). (it loads for example on the operation memory 35)

[0103] RMP acquisition place information is described in URL (Uniform Resource Locator) form for example in right processing metadata. In such a case the content reception machine 30 carries out resource access to the server directed by URL via a TCP/IP network like the Internet by network interface 37 course. An applicable RMP module is downloadable according to transfer protocol such as HTTP (Hyper Text Transfer Protocol) or FTP (File Transfer Protocol).

[0104] In [as a result of installing a new software RMP module] the content reception machine 30 top it can operate as RMP specification description described as right processing metadata and contents processing of a decoding of enciphered content an external output as reproduction contents the hard disk drive 33A storing in a removable media etc. can be performed now.

[0105] Then after carrying out connection establishment to a control center and performing accounting about content purchase based on RMP specification description (Step S3) contents playback is performed (step S4) and this whole manipulation routine is ended.

[0106] As a modification which constitutes a RMP module as a software module CPU 32 (or other arithmetic processing units) analyzes RMP specification description in right processing metadata and it may be made to generate a desired software RMP module automatically by content reception machine 30 inside.

[0107] In drawing 6 procedure for generating a software RMP module automatically by content reception machine 30 inside is illustrated in the form of a flow chart. Hereafter according to this flow chart automatic generation processing of a software RMP module is explained.

[0108] When starting reproduction of contents accumulated in the hard disk drive 33A corresponding right processing metadata is similarly read from the hard disk drive 33A and RMP ID of a RMP module is acquired (Step S11). And this RMP ID confirms whether it is in agreement with it of a RMP module loaded to the present operation memory 35 (Step S12).

[0109] When a RMP module of contents which RMP ID hits namely reproduces after this is already loaded on the operation memory 35 then after carrying out connection establishment to a control center and performing accounting about content purchase based on RMP specification description (Step S13) contents playback is performed (Step S14) and this whole manipulation routine is ended.

[0110]On the other handwhen RMP ID does not hitinformation about RMP specification description is acquired from right processing metadata (Step S15). Subsequentlyit is confirmed whether KOMPYUTESHON power (for examplecount ability which CPU32 has) on the content reception machine 30 is sufficient for generating a RMP module (Step S16).

[0111]After displaying the message of the purport that contents are unreproducible in the case of KOMPYUTESHON insufficient power (Step S19)abnormal termination of this manipulation routine is carried out.

[0112]On the other handwhen KOMPYUTESHON power is enoughfurtherRMP specification description is decoded (Step S17)and RMP is set up on the operation memory 35 (Step S18). As a result of setting up RMP newlyit operates as the RMP specification description described as right processing metadata on the content reception machine 30Contents processing of a decoding of enciphered contentthe external output as reproduction contentsthe hard disk drive 33Astoring in a removable mediaetc.etc. can be performed now.

[0113]Thenafter carrying out connection establishment to a control center and performing accounting about content purchase based on RMP specification description (Step S13)contents playback is performed (Step S14) and this whole manipulation routine is ended.

[0114]When a RMP module is constituted as a hardware moduleit cannot comparewhen it mounts a module with softwareand cannot transpose to other RMP modules easily. In such a casein the server sidestructure which is transposed to RMP corresponding to a receiver may be provided. For examplea content reception machine side is asked to a server by ID of contentsand requests conversion of contents. If right processing conditions are readyit can change into predetermined RMPand they are the contents (.) after conversion. or the thing for which the same contents are prepared beforehand -- it may be -- a decoding and reproducing of contents are realizable by downloading to the content reception machine of a requesting agency. [to wish]

[0115]Subsequentlyan embodiment at the time of applying this invention to a contents distribution system with which a content provider performs contents distribution using satellite broadcasting is described.

[0116]In drawing 7rough composition of the contents distribution system 100 is illustrated. The contents distribution system 100 shown in the figureThe content provider 200 who consists of a program production company or a commission broadcasting organization who makes and provides contentsIt comprises the satellite broadcasting trust broadcasting organization (it is only hereafter considered as a "broadcasting station") 300 who distributes contents made and provided by satellite broadcasting wavesand the satellite broadcasting receiver (it is only hereafter considered as a "content reception machine") 400 corresponding to contents distribution installed in each ordinary home. Generally the content reception machine

400 is connected with Television Sub-Division 450 for an image and voice response (TV).

[0117]Between the content provider 200 and the broadcasting station 300consignment contract about contents work and offer is signedandas for work (or it acquired from external content provider) contents the broadcasting station 300 is provided with the content provider 200. The broadcasting station 300 enciphers contentsputs this on satellite broadcasting wavesand distributes it towards the content reception machine 400 domestic [each].

[0118]The content provider 200 may contract with the organization of a settlement-of-accounts speciality [like the control center 202 of the independent exterior which manages a contents fee] whose program production company 201 as a contents work entrepreneur is. In such a casethe content provider 200 leaves management of the key which enciphers contents to the control center 202and the control center 202 passes contents selling information.

[0119]The control center 201 may be interlocked with further the external certificate authority 250 and other settlement-of-accounts organizations. The control center 202 is connected periodically or irregularly between each content reception machines 400and the key information for making enciphered content available to the content reception machine 400 is distributed. The content reception machine 400 decodes the enciphered content which received by the broadcasting satellite 301 course based on RMP specification description using the distributed key informationand appropriates it for the use. The content reception machine 400 contains a large capacity external storage like a hard disk driveand can accumulate the contents which received.

[0120]To the control center 201accounting informationsuch as a reproduction log of contentsis remitted from the content reception machine 400. The user of the content reception machine 400 side should just settle the charge amount of a contents use count to a control center every monthfor example. Anysuch as cash paymenttransfer to a predetermined financial institutionprepayment by a prepaid cardcredit settlement by a credit cardreal-time settlement by a debit cardand use of electronic moneymay be sufficient as means of settlement.

[0121]In drawing 8the composition in the broadcasting station 300 which performs contents work and distribution is illustrated typically. Hereafterstructuresuch as encryption at the time of contents distributionis explainedreferring to drawing 8.

[0122]The contents encryption section 311 enciphers contents provided by the content providersuch as an image and musicusing the contents key (contents key) Kc. Howeverthe encryption and other right processings in accordance with the RMP specification description as which it was decided upon the contents provided by the content provider in the content provider shall be applied.

[0123]The contents key encryption section 312 enciphers the contents key Kc using the distribution key (distribution key) KD.

[0124]The multiplexer 313 multiplexes an enciphered content key inputted as

enciphered content inputted from the contents encryption section 311 from the contents key encryption section 312 and generates transport stream TS (Transport Stream). A transport stream is a data stream by which metadata and an enciphered content key were added to enciphered content.

[0125] In the content reception machine 400, limited reception of the CAS scrambler 314 is carried out — it should make — a transport stream — scramble — that is a scrambling treatment is carried out. It can be enciphered by an enciphering device which is not illustrated for example and contract information a scramble key etc. In CAS can be put on a broadcast wave and can be transmitted to the content reception machine 400 side.

[0126] Composition of an example 400A of a content reception machine which receives contents distributing conveyed as a broadcast wave is typically shown in drawing 9. Once the content reception machine 400A shown in the figure accumulates contents which received in predetermined local memory units such as a hard disk it is a type which opts for the purchase of contents. Hereafter the content reception machine 400A is explained referring to the figure.

[0127] The CAS descrambler 411 carries out the descrambling of the data received by the front end which is not illustrated using the scramble key acquired from the broadcasting station 300 side and reproduces a transport stream.

[0128] The demultiplexer 412 divides a transport stream into enciphered content and an enciphered content key. These are once accumulated in the hard disk drive 413A after separation with the state before right processing.

[0129] The RMP module 420 may be mounted with which form of the hardware module or the software module. When purchasing the contents accumulated in the hard disk drive 413A, corresponding right processing metadata is read first. RMP identification information (RMP ID) is detected from the inside and a suitable RMP module assumes that it is operating selectively.

[0130] It connects with the control center (or the user account is acquired) 202 which signed the contract about content purchase and the RMP module 420 purchases the distribution key KD of contents. The contents key decoding section 421 takes out an enciphered content key from right processing metadata and decrypts this with the distribution key KD and obtains the contents key Kc. The following contents key re-encryption section 422 re-enciphers the contents key Kc using the key Ks for contents storage (storage key) specified by the RMP module 420.

[0131] Purchased enciphered content is moved to the hard disk drive 413B from the hard disk drive 413A with a re-enciphered contents key. However, the hard disk drives 413A and 413B do not need to be isolated—system units physically and may have a storage area (for example partition) divided a right processing front (before purchase) and after right processing (after purchase) within the same hard disk.

[0132] The RMP module 420 accumulates processing logs such as the purchase of the distribution key KD for purchase contents and movement of purchase contents as

billing data. And it connects with the control center 202 periodically or irregularly and billing data is transmitted.

[0133] Composition of other examples 400B of a content reception machine which receives contents distributing conveyed as a broadcast wave is typically shown in drawing 10. Once the content reception machine 400B shown in the figure accumulates contents which received in local memory unit such as a hard disk it is a type reproduced in contents. The content reception machine 400B functions also as playback equipment of enciphered content purchased and accumulated by the content reception machine 400A mentioned above. Hereafter the content reception machine 400B is explained referring to the figure.

[0134] The contents enciphered in the hard disk drive 433 using the contents key Kc specified by the RMP module 440. The enciphered content key enciphered with the key Ks for contents storage (storage key) specified by the RMP module 440 is stored.

[0135] At the time of content purchase the contents key decoding section 441 reads an enciphered content key applicable from the hard disk drive 433 and decrypts it using the storing key Ks in which this was specified and obtains the contents key Kc.

[0136] The contents decoding section 442 reads enciphered content to purchase from the hard disk drive 433 and decrypts it using the contents key Kc which had this decrypted and reproduces contents such as the original image or music.

[0137] After the APS treating part 443 applies contents protecting processing such as a macro vision and CGMS-A to analog output signals such as a video signal it is sent out to output unit such as Television Sub-Division (not shown) as reproduction contents.

[0138] According to the content reception machine 400A as shown in drawing 9 and drawing 10 the content provider can distribute contents with the encryption system which became independent of CAS. That is since it is a contents distribution system independent of CAS accounting to content purchase can be performed on the common platform over different CAS (a different broadcasting organization). In this case CAS is only a distribution channel of mere contents. Contents are accumulated in a local memory unit like a hard disk drive in the state enciphered. Since the key for solving contents is locked and changed into the storing key Ks from the contents key Kc at the time of purchase it is renewable on the same content reception machine 400A after that at any time. Since the log for charging at the time of content purchase processing is created and it is transmitted to the control center 202 periodically or irregularly fee collection and settlement of accounts can be ensured to a contents user.

[0139] In the content reception machine 400A as shown in drawing 9 in the form of the flow chart shows an example of the procedure for accumulating receiving contents in the hard disk drive 413A to drawing 11. Fundamentally receiving contents are accumulated still in the state before right processing. Hereafter the accumulation processing of contents is explained according to this flow chart.

[0140]First it is confirmed whether the program to reserve by the user of the content reception machine 400A was decided (Step S21). (that is reservation setting carried out or not?)

[0141]When the program to reserve is already decided if it is digital broadcasting for example EPG (Electric Program Guide: electronic program guide) will be taken out of the data for data broadcasting and the program which should be reserved based on EPG is chosen (Step S22). And time (televising time zone) a channel etc. which should be reserved are set up (Step S23).

[0142]Subsequently a predetermined search engine makes auto select of the program which suited preference based on a preference input (Step S24) from a user (Step S25). And time (time zone) a channel etc. which should be reserved are set up (Step S26).

[0143]It answers that reached at reservation start time or selected program ID was received and automatic storage of receiving contents to a hard disk drive is performed (Step S27).

[0144]Composition of other examples 400C of a content reception machine which receives contents distributing conveyed as a broadcast wave is typically shown in drawing 12. A CAS module for satellite broadcasting in which the content reception machine 400C shown in the figure was IC-card-ized That is once accumulating contents which built in a BS-CAS IC card and received in a hard disk drive it is a type which carries out limited reception of the satellite broadcasting and views and listens to it based on a CAS system. Hereafter the content reception machine 400C is explained referring to the figure.

[0145]Data contents received by front end which is not illustrated are before right processing and are accumulated in a mass storage device like the hard disk drive 453 temporarily with the state where scramble processing was carried out by CAS.

[0146]Right processing of receiving contents is performed by the RMP module 460. The RMP module 460 may be mounted with which form of a hardware module or a software module. When purchasing contents accumulated in the hard disk drive 453 corresponding right processing metadata is read RMP identification information (RMP ID) is detected and a suitable RMP module assumes that it is operating selectively. A CAS module provided as an IC card constitutes some RMP modules 460 from an example of a graphic display.

[0147]When reproducing accumulated contents applicable right processing metadata is read from the hard disk drive 453.

[0148]In right processing metadata ECM (Entitlement Control Message) and EMM (Entitlement Management Message) are contained. ECM enciphers the scramble key Ksc for canceling CAS scramble. EMM enciphers a work key for solving ECM with contractual coverage and messages such as a contract term.

[0149]The decoding part 462 decodes EMM using the master key Km currently recorded on the BS-CAS IC card and acquires a work key and contract information.

Subsequently the decoding part 461 decodes ECM using a work key and obtains the scramble key Ksc.

[0150] The judgment part 464 verifies the justification of the content reception machine 400C based on the contract information acquired in the decoding part 462. When it judges with it being just the scramble key Ksc is supplied to the decoding part 465.

[0151] Based on CAS scramble processing of the receiving contents accumulated in the hard disk drive 453 is carried out by systemssuch as Multi2. The decoding part 465 takes out contents to reproduce namely view and listen from the hard disk drive 453 and carries out descrambling processing using the scramble key Ksc.

[0152] After the APS treating part 466 applies contents protecting processingssuch as a macro vision and CGMS-A to analog output signalssuch as a video signal it is sent out to output unitssuch as Television Sub-Division (not shown) as reproduction contents.

[0153] On the other hand the contract information acquired in the decoding part 462 is accumulated in the PPV data storing part 463. It connects with the control center 202 periodically or irregularly and the RMP module 460 transmits PPV data. The control center 202 can perform accounting to a contents user based on PPV data.

[0154] According to composition of the content reception machine 400D shown in drawing 12 CAS can be used for fee collection of accumulation contents as it is.

Contents enciphered according to CAS are accumulated in a hard disk drive while it had been enciphered by them. EMM and ECM can be solved with the master key Km used by CAS and accumulation contents can be solved. In that case it records having solved a code as a fee collection log. By transmitting such a fee collection log to a control center periodically or irregularly fee collection can be ensured to a contents user.

[0155] Composition of other examples 400D of a content reception machine which receives contents distributing conveyed as a broadcast wave is typically shown in drawing 13. A CAS module for satellite broadcasting in which the content reception machine 400D shown in the figure was IC-card-ized That is after building in a BS-CAS IC card carrying out limited reception of the satellite broadcasting based on a CAS system and performing a CAS descrambling it is a type which is enciphered again and accumulated in a hard disk drive. Hereafter the content reception machine 400D is explained referring to the figure.

[0156] Right processing of receiving contents is performed by the RMP module 480. The RMP module 480 may be mounted with which form of a hardware module or a software module. When contents are received from a front end section (not shown) right processing metadata is read RMP identification information (RMPID) is detected and a suitable RMP module assumes that it is operating selectively. A CAS module provided as an IC card and a secure module which protects contents accumulated in a hard disk drive constitute some RMP modules 480 from an example

shown in the figure. A secure module performs re-encryption processing of contents accumulated in a hard disk drive and code release processing at the time of reproduction.

[0157] Right processing metadata is inputted into a CAS module, i.e. a BS-CAS IC card among data contents received by front end which is not illustrated.

[0158] In right processing metadata ECM (Entitlement Control Message) and EMM (Entitlement Management Message) are contained. The decoding part 482 decodes EMM using the master key Km currently recorded on a BS-CAS IC card and acquires a work key and contract information. Subsequently the decoding part 481 decodes ECM using a work key and obtains the scramble key Ksc. Contract information acquired in the decoding part 482 is accumulated in the PPV data storing part 483.

[0159] The judgment part 484 verifies the justification of the content reception machine 400D based on contract information acquired in the decoding part 482. When it judges with it being just the scramble key Ksc is supplied to the decoding part 485.

[0160] The decoding part 485 carries out descrambling processing of the receiving contents using the scramble key Ksc and outputs them to a secure module.

[0161] Within a secure module the encryption section 487 enciphers contents after a CAS descrambling again using the contents storage key Kst peculiar to the content reception machine 400D and stores in the hard disk drive 473.

[0162] In reproducing, namely viewing and listening to contents accumulated in the hard disk drive 473, enciphered content is read from the hard disk drive 473 and it decrypts using the contents storage key Kst by the decoding part 488. And after the APS treating part 489 applies contents protecting processing, such as a macro vision and CGMS-A to analog output signals, such as a video signal, it is sent out to output units, such as Television Sub-Division (not shown), as reproduction contents.

[0163] Within a secure module, right processing metadata is taken out from contents after CAS descrambling processing and it is accumulated as billing data.

[0164] The RMP module 480 is connected to the control center 202 periodically or irregularly and the PPV data stored by the CAS module and the billing data accumulated by the secure module are transmitted. The control center 202 can perform accounting to a contents user based on PPV data.

[0165] According to the content reception machine 400D of composition as shown in drawing 13, the contents distributed according to a CAS system can be enciphered again and it can accumulate in a hard disk drive. In the case of re-encryption, it enciphers with the contents storage key Kst of key structure which is different in the scramble key Ksc used by CAS. In reproducing the enciphered content accumulated in the hard disk drive, whenever it reproduces a fee collection log is generated and it transmits to the control center 202 periodically or irregularly and performs fee collection to a contents user. It can unite with a RMP module and CAS can also be constituted.

[0166] [Supplement] It has explained in detail about this invention referring to a

specific embodiment above. However it is obvious that a person skilled in the art can accomplish correction and substitution of this embodiment in the range which does not deviate from the summary of this invention. That is with the form of illustration this invention has been indicated and it should not be interpreted restrictively. In order to judge the summary of this invention the column of the Claims indicated at the beginning should be taken into consideration.

[0167]

[Effect of the Invention] As a full account was given above according to this invention the outstanding content reception equipment and contents receiving method with which a specific user can receive suitably the pay content distributed in the form that a movie, music, etc. were enciphered can be provided.

[0168]. According to this invention the enciphered content which contents work and providing agent, such as a movie and music distribute via brokers, such as a broadcasting organization and an Internet Service Provider, is suitably receivable. Outstanding content reception equipment and contents receiving method can be provided.

[0169] According to this invention contents work and the providing agent itself can provide the outstanding content reception equipment and contents receiving method which can receive suitably the contents which distribute fee collection security, etc. about contents use with a controllable form.

[0170] According to this invention the outstanding content reception equipment and contents receiving method which can respond to two or more RMP (Right Management & Protection) systems upon which it is decided for every contents distribution system can be provided.

[0171] It becomes unnecessary according to the content reception equipment and the contents receiving method concerning this invention to be able to respond to several different contents distribution systems using one set of a content reception machine and to prepare apparatus such as a receiver for every distribution system. Among each contents work and offer / distribution entrepreneur the argument involving standardization of contents distribution systems such as RMP specification description can be calmed down. The compatibility and flexibility of contents distributing between each contents work and offer / distribution entrepreneur can be raised. Convenience increases in a contents user.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a figure showing the conceptual composition of a RMP module.

[Drawing 2] Two or more hardware RMP modules which mounted different RMP specification are prepared and it is a figure showing typically the composition of the

content reception machine of the form changed and used for the hardware RMP module which suits for every receiving contents.

[Drawing 3] Two or more hardware RMP modules which mounted different RMP specification are prepared and it is a figure showing typically other examples of composition of the content reception machine 20 of the form changed and used for the hardware RMP module which suits for every receiving contents.

[Drawing 4] It is a figure showing typically other examples of composition of the content reception machine 30 of the form which downloads the software module which constitutes a RMP module as a software module and suits for every receiving contents from a predetermined server.

[Drawing 5] It is the flow chart which showed the procedure for downloading a RMP module to the content reception machine 30.

[Drawing 6] It is the flow chart which showed the procedure for generating a software RMP module automatically by content reception machine 30 inside.

[Drawing 7] It is a figure showing the rough composition of a contents distribution system.

[Drawing 8] It is a figure showing typically the composition in the broadcasting station which performs contents work and distribution.

[Drawing 9] It is a figure showing typically the composition of an example 400A of a content reception machine which receives the contents distributing conveyed as a broadcast wave.

[Drawing 10] It is a figure showing typically the composition of other examples 400B of the content reception machine which receives the contents distributing conveyed as a broadcast wave.

[Drawing 11] In the content reception machine 400A shown in drawing 9 it is the flow chart which showed an example of the procedure for accumulating receiving contents in the hard disk drive 413A.

[Drawing 12] It is a figure showing typically the composition of other examples 400C of the content reception machine which receives the contents distributing conveyed as a broadcast wave.

[Drawing 13] It is a figure showing typically the composition of other examples 400C of the content reception machine which receives the contents distributing conveyed as a broadcast wave.

[Drawing 14] It is a figure showing the general-view composition of the contents distribution system of a CAS base.

[Explanations of letters or numerals]

10 -- A content reception machine 11 -- Front end section

12 -- A CAS treating part 13A 13B -- Hard disk drive

14 -- RMP identification part

20 -- A content reception machine 21 -- Front end section

23 -- A hard disk drive 24 -- RMP identification part

25 -- Decoder output equipment
30 -- A content reception machine31 -- Front end section
32 -- CPU33A33B -- Hard disk drive
34 -- A RMP identification part35 -- Operation memory
36 -- Decoder output equipment37 -- Network interface
200 -- Content provider
201 -- A program production company (commission broadcasting organization)202 --
Control center (settlement-of-accounts organization)
250 -- Certificate authority
300 -- A broadcasting station (satellite broadcasting trust broadcasting
organization)301 -- Broadcasting satellite
311 -- A contents encryption section312 -- Contents key encryption section
313 -- A multiplexer314 -- CAS scrambler
400 -- Content reception machine (satellite broadcasting receiver corresponding to
contents distribution)
411 -- A CAS descrambler412 -- Demultiplexer
413A413B -- Hard disk drive
420 -- A RMP module421 -- Contents key decoding section
422 -- Contents key re-encryption section
433 -- A hard disk drive440 -- RMP module
441 -- A contents key decoding section442 -- Contents decoding section
443 -- APS treating part
453 -- A hard disk drive460 -- RMP module
461 -- A decoding part462 -- Decoding part
463 -- A PPV data storing part464 -- Judgment part
465 -- A decoding part466 -- APS treating part
473 -- A hard disk drive480 -- RMP module
481 -- A decoding part482 -- Decoding part
483 -- A PPV data storing part484 -- Judgment part
485 -- A decoding part487 -- Encryption section
488 -- A decoding part489APS treating part

【特許請求の範囲】

【請求項1】 所定の権利管理・保護 (Right Management & Protection: RMP) 方式に則って配信されるコンテンツを受信するコンテンツ受信装置であって、配信コンテンツを受信するコンテンツ受信手段と、受信コンテンツの権利管理・保護方式を識別する識別手段と、前記識別手段による識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理手段と、を具備することを特徴とするコンテンツ受信装置。

【請求項2】 権利管理・保護方式は、コンテンツの暗号化方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、APS (Analog Protection System: マクロビジョンやCGMS (Copy Generation Management System) など)、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目を規定することを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項3】 複数種類の権利管理・保護モジュールを備え、

前記権利処理手段は、前記識別手段による識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行う、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項4】 権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得手段を備え、

前記権利処理手段は、前記識別手段による識別結果に基づいて前記権利管理・保護モジュール取得手段を介して外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項5】 権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成手段を備え、

前記権利処理手段は、前記権利管理・保護モジュール生成手段によって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項6】 コンテンツを蓄積するコンテンツ蓄積手段を含むことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項7】 コンテンツを蓄積するコンテンツ蓄積手段を含み、

前記権利処理手段による権利処理前のコンテンツを前記コンテンツ蓄積手段に格納する、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項8】 コンテンツを蓄積するコンテンツ蓄積手段を含み、

前記権利処理手段による権利処理後のコンテンツを前記

コンテンツ蓄積手段に格納する、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項9】 前記コンテンツ受信手段は所定の鍵で暗号化された形式で配信されるコンテンツを受信し、コンテンツを蓄積するコンテンツ蓄積手段をさらに含み、

前記権利処理手段は、受信した暗号化コンテンツを復号化し、他の鍵で再暗号化した後にコンテンツ蓄積手段に格納する、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項10】 前記コンテンツ受信手段は、所定の鍵で暗号化された形式で配信されるコンテンツ、並びに該鍵を暗号化した暗号化鍵を受信し、コンテンツを蓄積するコンテンツ蓄積手段をさらに含み、

前記権利処理手段は、受信した暗号化鍵を復号化し、他の鍵で再暗号化した後に暗号化コンテンツとともにコンテンツ蓄積手段に格納する、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項11】 前記権利処理手段は、受信コンテンツの権利処理のログを蓄積することを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項12】 前記権利処理手段は、権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってAPS (Analog Protection System) 処理して外部出力する、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項13】 前記権利処理手段は、権利処理後のコンテンツを暗号化して外部出力することを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項14】 所定の権利管理・保護 (Right Management & Protection: RMP) 方式に則って配信されるコンテンツを受信するコンテンツ受信方法であって、配信コンテンツを受信するコンテンツ受信ステップと、受信コンテンツの権利管理・保護方式を識別する識別ステップと、

前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とするコンテンツ受信方法。

【請求項15】 権利管理・保護方式は、コンテンツの暗号化方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、APS (Analog Protection System: マクロビジョンやCGMS (Copy Generation Management System) など)、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目を規定することを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項16】 複数種類の権利管理・保護モジュールを備え、

前記権利処理ステップでは、前記識別ステップによる識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行う、ことを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項17】前記識別ステップによる識別結果に基づいて、該当する権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得ステップをさらに備え、

前記権利処理ステップでは、前記権利管理・保護モジュール取得ステップにより外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項18】権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成ステップをさらに備え、

前記権利処理ステップでは、前記権利管理・保護モジュール生成ステップによって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項19】受信したコンテンツを蓄積するコンテンツ蓄積ステップを含むことを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項20】前記権利処理ステップによる権利処理前のコンテンツを格納するコンテンツ蓄積ステップを含むことを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項21】前記権利処理ステップによる権利処理後のコンテンツを格納するコンテンツ蓄積ステップを含むことを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項22】前記コンテンツ受信ステップでは所定の鍵で暗号化された形式で配信されるコンテンツを受信し、

前記権利処理ステップにおいて復号化した受信コンテンツを他の鍵で再暗号化した後に格納するコンテンツ蓄積ステップを備える、ことを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項23】前記コンテンツ受信ステップでは、所定の鍵で暗号化された形式で配信されるコンテンツ、並びに該鍵を暗号化した暗号化鍵を受信し、

前記権利処理ステップにおいて復号化した鍵を他の鍵で再暗号化した後に暗号化コンテンツとともに格納するコンテンツ蓄積ステップを備える、ことを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項24】前記権利処理ステップにおける受信コンテンツの権利処理のログを蓄積するログ蓄積ステップを備えることを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項25】前記権利処理ステップによる権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってAPS (Analog Protection System) 処理して外部出力する外部出力ステップを備える、ことを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項26】前記権利処理ステップによる権利処理後のコンテンツを暗号化して外部出力する外部出力ステップを備える、ことを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項27】所定の権利管理・保護 (Right Management & Protection: RMP) 方式に則って配信されるコンテンツの受信処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、配信コンテンツを受信するコンテンツ受信ステップと、受信コンテンツの権利管理・保護方式を識別する識別ステップと、

前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とする記憶媒体。

【請求項28】それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、権利管理・保護方式の識別情報を含んだ要求にตอบสนองして、該当する権利管理・保護モジュールを送信する手段と、を備えることを特徴とするサーバ。

【請求項29】それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、識別情報に基づく問合せにตอบสนองして、該当する権利管理・保護モジュールを用いてコンテンツを変換する手段と、を具備することを特徴とするサーバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、放送波やネットワークなどを介して配信されるコンテンツを受信するコンテンツ受信装置及びコンテンツ受信方法に係り、特に、映画や音楽などの暗号化された形式で配信される有料コンテンツを特定の利用者が受信するコンテンツ受信装置及びコンテンツ受信方法に関する。

【0002】更に詳しくは、本発明は、映画や音楽などのコンテンツ制作・提供者が放送事業者やインターネット・サービス・プロバイダなどの仲介業者を介して配信する暗号化コンテンツを受信するコンテンツ受信装置及びコンテンツ受信方法に係り、特に、コンテンツ制作・提供者自身がコンテンツ利用に関する課金やセキュリティなどを制御可能な形態で配信するコンテンツを受信するコンテンツ受信装置及びコンテンツ受信方法に関する。

【0003】

【従来の技術】 昨今の情報技術の革新に伴い、映像や音楽など、さまざまなメディアがデジタル化されたコンテンツとしてコンピュータなどの情報機器上で取り扱われるようになってきている。さらに、情報通信技術の発達により、これらコンテンツを、衛星や地上波などの放送、あるいはインターネットのような広域的なネットワークを利用して、配信することができる。

【0004】 映像コンテンツや音楽コンテンツの配信は一部で既に実施されている。コンテンツ配信技術によれば、旧来の商品流通経路や物理的な媒体を省略することができる。また、遠隔地の消費者であっても、所望の映像・音楽ソフトを容易に入手することができる。また、コンテンツ制作・提供業者側の立場では、迅速且つ効率的なコンテンツ販売によってより高い利益をあげることに、コンテンツ制作意欲が増し、業界全体の発展にもつながる。

【0005】 例えば、テレビ受信機が大容量のハード・ディスク装置を内蔵していることを前提としたサーバ型・蓄積型の放送システムにおいては、映画などのコンテンツを、放送局やその他のコンテンツ配信業者において暗号化して配信し、コンテンツ購入者すなわち視聴者に対して暗号解読用の鍵を配布時に課金することによって確実に利益を確保することができる。

【0006】 このようなコンテンツ受信形式のことをCAS (Conditional Access System (限定受信)) 方式とも呼ぶ。図14には、CASベースのコンテンツ配信システムの概観構成を図解している。

【0007】 図面に示すコンテンツ配信システムでは、映像や音楽などの配信用コンテンツを制作又は提供するコンテンツ・プロバイダと、コンテンツ・プロバイダが提供するコンテンツを、放送波やネットワークを経由して消費者に配信するコンテンツ配信事業者と、コンテンツを受信する消費者すなわち一般ユーザの3者で構成される。

【0008】 コンテンツ配信事業者は、例えば、BS (Broadcasting Satellite: 放送衛星) CS (Communication Satellite: 通信衛星) など放送衛星を利用した放送事業者、地上波を利用した放送事業者、あるいは、インターネットへの接続サービス並びにインターネット上の各種情報コンテンツ提供サービスを運営するインターネット・サービス・プロバイダなどで構成される。

【0009】 一般ユーザは、例えば自宅内に配信コンテンツを受信するコンテンツ受信機を配置している。放送波を介したコンテンツを受信するコンテンツ受信機は、例えばSTB (Set Top Box) のようなテレビ受信機でよい。また、インターネット経由でコンテンツを受信するコンテンツ受信機は、例えば、パーソナル・コンピュータ (PC) のような一般的な計算機システムでよい。コンテンツ受信機は、ハード・ディスク装置を内蔵し、

長時間すなわち大量の映像・音楽コンテンツを蓄積可能な蓄積型放送対応受信機であることが好ましい。

【0010】 コンテンツ受信機が放送波を介してコンテンツを受信するためには、各放送事業者毎に対応したCAS (限定受信) カードを装備しておく必要がある。また、インターネット経由でコンテンツを受信するためには、所定のインターネット・サービス・プロバイダからあらかじめユーザ・アカウント (利用者資格) を取得するとともに、コンテンツ購入時に最善のアクセス・ポイントを介してインターネット接続する必要がある。

【0011】 放送事業者がコンテンツ配信に要する費用や利益を回収するためには、例えばCASカード (あるいはCASを内蔵した受信機) 購入を利用すればよい。また、インターネット・サービス・プロバイダがコンテンツ配信に要する費用や利益を回収するためには、例えば、月々支払われる会費にコンテンツ利用料相当額を上乗せすればよい。但し、CASシステムやユーザ・アカウントによる課金方式は、コンテンツ配信事業者が個々の消費者すなわちコンテンツ利用者に対する課金を制御することを目的とするものであり、コンテンツ・プロバイダの制御下ではない。言い換えれば、コンテンツ・プロバイダは、コンテンツ配信事業者車体のCASなどを利用して、自らの利益を確保することはできない。

【0012】 コンテンツ・プロバイダが一般消費者からコンテンツ利用料を徴収するためには、コンテンツ・プロバイダ自身がコンテンツ課金、セキュリティ、著作権保護などのコンテンツ提供方式 (以下では、RMP (Right Management & Protection) と呼ぶ) を策定することが挙げられる。RMPの中には、より具体的に、暗号化の方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、APS (Analog Protection System: マクロビジョンやCGMS (Copy Generation Management System) など)、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目が含まれている。コンテンツの利用者・消費者側では、コンテンツ・プロバイダに対応するRMPモジュールを実装したコンテンツ受信機を用意することで、コンテンツ・プロバイダを供給源とする配信コンテンツを成功裏に購入し、利用すなわち視聴することができる。また、管理センタのようなコンテンツ・プロバイダ外の決済機関に対して課金情報の一括管理を委ねるようにしてもよい。

【0013】 しかしながら、コンテンツ課金、セキュリティ、著作権保護に関するRMP方式は、一般に、各コンテンツ・プロバイダが提供するコンテンツ配信システム毎に区々に策定するのが現状である。複数の方式が混在する環境下では、同じ音楽コンテンツ配信、映画コンテンツ配信であっても、コンテンツ配信システムが違えば同じコンテンツ受信機上では復号化できない、す

なわちコンテンツを利用できないという事態に陥る。

【0014】例えば、コンテンツ利用者が複数のコンテンツ・プロバイダすなわち配信システムからコンテンツを購入しようとする、各配信システム毎にコンテンツ受信機のハードウェア又はソフトウェアを用意しなければならず、利用者に不便であったり、あるいは余計な出費が必要となる。また、コンテンツ購入方法が面倒であることの帰結として、利用者のコンテンツ買い控えが生じると、コンテンツ提供・配信事業の利益が伸び悩み、事業全体が沈滞化してしまうことになりかねない。

【0015】

【発明が解決しようとする課題】本発明の目的は、映画や音楽などの暗号化された形式で配信される有料コンテンツを特定の利用者が好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【0016】本発明の更なる目的は、映画や音楽などのコンテンツ制作・提供者が放送事業者やインターネット・サービス・プロバイダなどの仲介業者を介して配信する暗号化コンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【0017】本発明の更なる目的は、コンテンツ制作・提供者自身がコンテンツ利用に関する課金やセキュリティなどを制御可能な形態で配信するコンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【0018】本発明の更なる目的は、各コンテンツ配信システム毎に策定される複数のRMP (Right Management & Protection) 方式に対応することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【0019】

【課題を解決するための手段及び作用】本発明は、上記課題を参照してなされたものであり、その第1の側面は、所定の権利管理・保護 (Right Management & Protection: RMP) 方式に則って配信されるコンテンツを受信するコンテンツ受信装置であって、配信コンテンツを受信するコンテンツ受信手段と、受信コンテンツの権利管理・保護方式を識別する識別手段と、前記識別手段による識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理手段と、を具備することを特徴とするコンテンツ受信装置である。

【0020】コンテンツの制作・提供者事業者は、RMPと呼ばれる権利管理・保護方式に従って暗号化などの保護された形式でコンテンツを配信する。一般に、コンテンツ制作・提供者事業者毎に区々の権利管理・保護方式を採用する。

【0021】本発明の第1の側面に係るコンテンツ受信

装置によれば、権利管理・保護方式の仕様を規定する書式のみを統一化するだけで、識別手段が受信コンテンツの権利管理・保護方式を識別して、権利処理手段は、該識別結果に基づいて該当する権利管理・保護方式を選択的に用いて受信コンテンツを権利処理することができる。

【0022】したがって、それぞれの権利管理・保護方式に対応した機能をあらかじめ用意しておくだけで、どの権利管理・保護方式に則ったコンテンツを受信した場合であっても、1台のコンテンツ受信機を用いて複数の異なるコンテンツ配信方式に対応することができる。すなわち同じコンテンツ受信機上でコンテンツを復号化して利用に供することができ、配信システム毎の受信機などの機器を用意する必要がなくなる。

【0023】また、各コンテンツ制作・提供・配信事業者間では、RMP仕様記述などのコンテンツ配信方式の規格化をめぐる争いを沈静化することができる。また、各コンテンツ制作・提供・配信事業者間における配信コンテンツの互換性や融通性を向上させることができる。また、コンテンツ利用者においては、利便性が高まる。

【0024】ここで言う権利管理・保護方式は、コンテンツの暗号化方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や報酬の伝送方式、記録メディア制御情報、相互認証の方式、APS (Analog Protection System: マクロビジョンやCGMS (Copy Generation Management System) など)、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目を規定するものである。

【0025】コンテンツ受信装置は、あらかじめ複数種類の権利管理・保護モジュールを備えておいてもよい。このような場合、前記権利処理手段は、前記識別手段による識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行うことができる。

【0026】あるいは、コンテンツ受信装置は、権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得手段を備えていてもよい。このような場合、前記権利処理手段は、前記識別手段による識別結果に基づいて前記権利管理・保護モジュール取得手段を用いて外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことができる。

【0027】あるいは、コンテンツ受信装置は、権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成手段を備えていてもよい。このような場合、前記権利処理手段は、前記権利管理・保護モジュール生成手段によって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことができる。

【0028】また、コンテンツ受信装置は、コンテンツを蓄積するコンテンツ蓄積手段を含んでいてもよい。例

えば、前記権利処理手段による権利処理前、あるいは権利処理後のコンテンツを前記コンテンツ蓄積手段に格納することができる。

【0029】前記コンテンツ受信手段が受信するコンテンツは、例えば、所定の鍵で暗号化されている。このような場合、前記権利処理手段は、受信した暗号化コンテンツを復号化し、他の鍵で再暗号化した後にコンテンツ蓄積手段に格納するようにしてもよい。このような構成により、権利処理後のコンテンツをさらに保護することができる。

【0030】また、前記コンテンツ受信手段が受信するコンテンツは、例えば、所定の鍵で暗号化された形式で配信されているとともに、さらに該鍵を暗号化した暗号化鍵も受信する。このような場合、前記権利処理手段は、受信した暗号化鍵を復号化し、他の鍵で再暗号化した後に暗号化コンテンツとともにコンテンツ蓄積手段に格納するようにしてもよい。このような構成により、権利処理後のコンテンツをさらに保護することができる。

【0031】また、前記権利処理手段は、受信コンテンツの権利処理のログを蓄積するようにしてもよい。このような場合、例えば、蓄積されたログを所定の決済機関に定期的にあるいは定期的に送信することにより、決済機関では正確な課金処理を行うことができる。

【0032】また、前記権利処理手段は、権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってAPS (Analog Protection System) 処理して外部出力するようにしてもよい。このような場合、権利処理後のビデオ再生信号などを保護することができる。

【0033】また、前記権利処理手段は、権利処理後のコンテンツを暗号化して外部出力するようにしてもよい。このような場合、例えばIEEE 1394のようなホーム・ネットワーク経由で他の情報機器にコンテンツを転送する場合や、LAN経由でパーソナル・コンピュータ (PC) のような計算機システムにコンテンツを送信してアプリケーションを用いて処理する場合であっても、コンテンツを保護することができる。

【0034】また、本発明の第2の側面は、所定の権利管理・保護 (Right Management & Protection: RMP) 方式に則って配信されるコンテンツを受信するコンテンツ受信方法であって、配信コンテンツを受信するコンテンツ受信ステップと、受信コンテンツの権利管理・保護方式を識別する識別ステップと、前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とするコンテンツ受信方法である。

【0035】本発明の第2の側面に係るコンテンツ受信方法によれば、権利管理・保護方式の仕様を規定する書式のみを統一化するだけで、識別ステップが受信コンテ

ンツの権利管理・保護方式を識別して、権利処理ステップでは、該識別結果に基づいて該当する権利管理・保護方式を選択的に用いて受信コンテンツを権利処理することができる。

【0036】前記権利処理ステップでは、前記識別ステップによる識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行うようにしてもよい。

【0037】あるいは、前記識別ステップによる識別結果に基づいて、該当する権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得ステップをさらに備えていてもよい。このような場合、前記権利処理ステップでは、前記権利管理・保護モジュール取得ステップにより外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことができる。

【0038】あるいは、権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成ステップをさらに備えていてもよい。このような場合、前記権利処理ステップでは、前記権利管理・保護モジュール生成ステップによって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことができる。

【0039】また、受信したコンテンツを蓄積するコンテンツ蓄積ステップを含んでもよい。例えば、前記権利処理ステップによる権利処理前、あるいは権利処理後のコンテンツを格納するようにしてもよい。

【0040】また、前記コンテンツ受信ステップでは所定の鍵で暗号化された形式で配信されるコンテンツを受信するような場合、前記権利処理ステップにおいて復号化した受信コンテンツを他の鍵で再暗号化した後に格納するコンテンツ蓄積ステップを備えていてもよい。

【0041】また、前記コンテンツ受信ステップでは、所定の鍵で暗号化された形式で配信されるコンテンツと、並びに該鍵を暗号化した暗号化鍵を受信するような場合、前記権利処理ステップにおいて復号化した鍵を他の鍵で再暗号化した後に暗号化コンテンツとともに格納するコンテンツ蓄積ステップを備えるようにしてもよい。

【0042】また、前記権利処理ステップにおける受信コンテンツの権利処理のログを蓄積するログ蓄積ステップを備えていてもよい。このような場合、例えば、蓄積されたログを所定の決済機関に定期的にあるいは定期的に送信することにより、決済機関では正確な課金処理を行うことができる。

【0043】また、前記権利処理ステップによる権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってAPS (Analog Protection System) 処理して外部出力する外部出力ステップを備えていてもよい。

【0044】また、前記権利処理ステップによる権利処

理後のコンテンツを暗号化して外部出力する外部出力ステップを備えていてもよい。

【0045】また、本発明の第3の側面は、所定の権利管理・保護(Right Management & Protection: RMP)方式に則って配信されるコンテンツの受信処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、配信コンテンツを受信するコンテンツ受信ステップと、受信コンテンツの権利管理・保護方式を識別する識別ステップと、前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とする記憶媒体である。

【0046】本発明の第3の側面に係る記憶媒体は、例えば、様々なプログラム・コードを実行可能な汎用性のコンピュータ・システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で物理的に提供する媒体である。このような媒体は、例えば、CD(Compact Disc)やFD(Floppy Disc)、MO(Magneto-Optical disc)などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク(ネットワークは無線、有線の区別を問わない)などの伝送媒体などを經由してコンピュータ・ソフトウェアを特定のコンピュータ・システムにコンピュータ可読形式で提供することも技術的に可能である。

【0047】このような記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働関係を定義したものである。換言すれば、本発明の第3の側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第1及び第2の各側面に係るコンテンツ受信装置及びコンテンツ受信方法と同様の作用効果を得ることができる。

【0048】また、本発明の第4の側面は、それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、権利管理・保護方式の識別情報を含んだ要求に応じて、該当する権利管理・保護モジュールを送信する手段と、を具備することを特徴とするサーバである。

【0049】また、本発明の第5の側面は、それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、識別情報に基づく問合せに応じて、該当する権利管理・保護モジュールを用いてコンテンツを交換する手段と、を具備することを特徴とするサーバである。

【0050】本発明のさらに他の目的、特徴や利点は、

後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0051】

【発明の実施の形態】以下に記述する本発明の実施形態では、各コンテンツ配信システム毎に策定される複数のRMPに対応することができるとするコンテンツ受信装置について説明する。

【0052】RMPは、Right Management & Protectionの略であり、TV Anytime Forumで用いられている概念である。放送やネットワークを介したコンテンツ配信事業において問題になるのが、コンテンツの不正利用やタダ見、タダ聴きである。この種の不正行為が横行すると、コンテンツ制作・提供・配信事業者の正当な利益が保証されず、事業の存亡にも関わる。言い換えれば、コンテンツの利用権利管理と保護が必要であり、RMPがこれを担う。

【0053】RMPには、より具体的には、暗号化の方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵額の伝送方式、記録メディア制御情報、相互認証の方式、APS(Analog Protection System: マクロビジョンやCGMS(Copy Generation Management System)など)、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目が含まれている。

【0054】これらの項目からなるRMPの仕様を規定する書式のみを統一し、各コンテンツ提供事業者は該仕様に則った形式で暗号化コンテンツや権利処理情報をコンテンツに入力すればよい。このような場合、コンテンツを受信し利用する消費者すなわちコンテンツ利用者側では、各々のRMP方式に対応した機能を複数用意しておくことにより、どのようなRMP方式に基づくコンテンツであっても、同じコンテンツ受信機上で復号化して利用に供することができる。

【0055】RMP仕様記述は、例えば、配信コンテンツに付随するメタデータの一部として記述することができる。以下では、メタデータのうちRMP仕様記述に関連する部分のことを「権利処理メタデータ」と呼ぶことにする。例えば、デジタル放送などの場合、放送番組本編に付随するデータ放送用データとしてメタデータを配信することができる。

【0056】図1には、RMPモジュールの概念構成を示している。RMPモジュールは、例えば、STB(Set Top Box)やその他の形態のコンテンツ受信機に内蔵して用いられ、所定のハードウェア又はソフトウェアのモジュールを用いて実装することができる。同図に示すように、RMPモジュールは、受信コンテンツに関するデータを入力を行うための幾つかのインターフェースを備えた構成となっている。

【0057】衛星波又は地上波などの放送を介して受信されたコンテンツ、あるいは、インターネットなどのネットワーク経由でダウンロードされたコンテンツは、メ

データとともに、ハード・ディスク装置などのような大容量蓄積装置内に格納される。RMPモジュールは、ハード・ディスク装置経由で、あるいはハード・ディスク装置を介さずに直接、権利処理前の状態で受信コンテンツを入力する。

【0058】映像や音楽などのコンテンツ本体はコンテンツ保護の目的で暗号化が施されている。したがって、暗号化コンテンツを解くための解読機能 (Decryptor) が必要であり、RMPモジュールは、規定された暗号アルゴリズムにより暗号化コンテンツを入力する暗号化コンテンツ入力用インターフェースを持つ。

【0059】また、各コンテンツに対応してメタデータが配信されるが、その中には、コンテンツに関する権利処理や必要な権利保護を示す情報、すなわち権利処理メタデータが含まれている。

【0060】権利処理メタデータには、コンテンツを解くための鍵種、コンテンツの購入条件、使用条件、解読されたコンテンツのコピー制御情報などが含まれる。RMPモジュールは、規定のフォーマットに従い権利処理や保護に関する情報を入力する権利処理メタデータの入力インターフェースを持つ。

【0061】配信コンテンツは、例えばコンテンツ鍵によって暗号化され、このコンテンツ鍵はさらに配信鍵 (Distribution Key) によって暗号化された形態で、暗号化コンテンツとともに伝送されてくる。RMPモジュール内には配信鍵が保持されており、この配信鍵を用いて暗号化されたコンテンツ鍵を解読し、さらに、解読されたコンテンツ鍵を用いて暗号化コンテンツを解読することができる。このような暗号化・伝送方式によれば、コンテンツ毎にコンテンツ鍵を変えながら安全にコンテンツ配信を行うことができる。また、RMPモジュールでは単一の配信鍵を保持することで暗号化コンテンツを解読して利用に供することができる。RMPモジュールの権利処理メタデータ入力インターフェースは、暗号化コンテンツ鍵を権利処理メタデータとして入力するようにしてもよい。

【0062】また、コンテンツ制作・提供事業者において策定するコンテンツ利用のための課金に関する仕様も、権利処理メタデータに含め、RMPモジュールの権利処理メタデータ入力インターフェースはこれを入力するようにしてもよい。

【0063】課金に関する仕様として、例えば、価格情報、使用条件 (1回毎の再生課金、あらかじめ再生可能な回数を規定した回数制限、所定の期日まで再生可能な期間制限など) などを規定することができる。

【0064】コンテンツ利用者に対する課金処理のために、管理センタのようなコンテンツ制作・提供・配信事業者以外の決済機関を設立してもよい。RMPモジュールは、このような管理センタに接続して、課金や決済に関するトランザクションを行うための課金処理インター

フェースを持つ。RMPモジュールは、例えば、ハード・ディスク装置上に蓄積されたコンテンツを再生する毎に課金ログを生成して、所定期間毎に管理センタに接続してログを送信する。これに対し、管理センタは、各コンテンツ利用者から送られてくるログに基づいて課金並びに決済処理を行うことができる。

【0065】RMPモジュールは、権利処理前の受信コンテンツを入力するための暗号化コンテンツ用インターフェースを備えていることは既に述べた通りである。RMPモジュールは、コンテンツの回数にわたる利用のために、権利処理後のコンテンツを再びハード・ディスク装置に蓄積するためのインターフェースや、コンテンツの永久・半永久保存のために、権利処理後のコンテンツをDVD (Digital Versatile Disc) などのリムーバブル・メディア上に格納するためのインターフェースを備えている。このような権利処理後のコンテンツ蓄積・再生用のインターフェースは、蓄積用コンテンツの暗号化や再生時における復号化などのメディアに対する制御や、メディアに対する認証の有無や認証方法などを規定することができる。

【0066】また、RMPモジュールは、受信コンテンツ、あるいはハード・ディスク装置やリムーバブル・メディアから読み出したコンテンツを、ディスプレイやその他の外部機器で再生するための外部出力インターフェースを備えている。図1に示す例では、ビデオ信号としてディスプレイ上に表示出力するためのアナログ出力インターフェースと、IEEE 1394などのホームネットワーク経由で外部機器にコンテンツを転送するためのデジタル出力インターフェースを備えている。アナログ出力インターフェースは、アナログ形式のコンテンツ保護のために、APS (Analog Protection System) などを採用する。APSには、マクロビジョンや、垂直帰線区間の所定の走査線にコピー制御情報を埋め込むCGMS (Copy Generation Management System) -A、SCMSなどが含まれる。また、デジタル出力インターフェースでは、送信コンテンツ暗号化の他、1394C Pのような認証バス・エンクリプションなどの制御を行うことができる。

【0067】また、権利処理後のコンテンツを転送して、パーソナル・コンピュータ (PC) のような情報処理機器上で所望のアプリケーションを用いた処理を行うことができる。図1に示す例では、RMPモジュールは、外部の情報処理機器にコンテンツを出力するためのホスト/アプリケーション用インターフェースを備えている。ホスト/アプリケーション用インターフェースは、送信コンテンツの暗号化などの制御を行う。

【0068】RMPモジュールは、専用のハードウェア・コンポーネントで実装することも、あるいは、汎用プロセッサ上で所定のプログラム・コードを実行することによっても実現可能である。RMPに関する仕様は、権

利処理メタデータとして、配信コンテンツに付随して配信・配布することができる（前述）。

【0069】RMP仕様記述フォーマットの一例を以下に示しておく。

【0070】

【数1】

```

RMP ID::=INTEGER{XXXXXXXX}
Contents Encryption Algorithm::=SEQUENCE{
    algorithm          3DES
    developer          Public
    download           URL

    key length         112
    key party          16
    key name           Content Key
}
Content Key Encryption Algorithm::=SEQUENCE{
    algorithm          DES
    developer          Public
    download           URL
    key length         56
    key party          8
    key name1          Distribution Key
    key name2          Storage Key
}
Distribution Key Encryption Algorithm::=SEQUENCE{
    algorithm          None
}
Storage Key Encryption Algorithm::=SEQUENCE{
    algorithm          None
}
Authentication Algorithm::=SEQUENCE{
    algorithm          DES
    developer          Public
    download           URL
    ECC parameter p    XXXXXXXXXXXXXXXX
    ECC parameter a    XXXXXXXXXXXXXXXX
    ECC parameter h    XXXXXXXXXXXXXXXX
    ECC parameter g    XXXXXXXXXXXXXXXX
    ECC parameter r    XXXXXXXXXXXXXXXX
    key length         224

    key party          0
}
Log Format::=SEQUENCE{
    log serial number   XXXXXXXX
    purchase date       yyyy:mm:dd
    purchase time       hh:mm:ss
    content ID          XXXXXXXXXXXX
    purchase condition   xxx
    purchase limitation  xxxxxx
    purchase price       xxxxxx
    copy permission     xx
}
... ..

```

【0071】上記で示したRMP仕様記述フォーマット

では、RMPの方式を識別するための識別情報(RMP ID)を冒頭に含む他、配信コンテンツを暗号化する暗号化アルゴリズム、配信コンテンツの暗号化に使用するコンテンツ・キーKsを暗号化する暗号化アルゴリズム、コンテンツ配信時に使用する配信キーKdを暗号化する暗号化アルゴリズム、配信コンテンツを蓄積するとき使用するストレージ・キーKst、相互認証に用いる認証アルゴリズム、ログを蓄積するためのフォーマットなどを規定することができる。暗号化方式としては、一般に、DES(Data Encryption Standard)やMulti2などが使用される。

【0072】RMPとしての仕様記述は、各コンテンツ制作・提供事業者毎に策定される。従来は、各コンテンツ配信システム毎にRMPを固定して利用していたので、複数のシステムからコンテンツの提供を受けるためには、新しいコンテンツ受信機を用意するなど余計な出費が必要であった。これに対し、本発明では、RMPの仕様記述、並びにRMPに入力するためのインターフェースを規定することにより、その仕様を解釈するか、又はその仕様と適合したRMPモジュールを入手することにより、同一のコンテンツ受信機上、複数のコンテンツ配信システムにおけるコンテンツ録画、暗号化などのセキュリティ方式、著作権保護方式に対応することができる。

【0073】本発明の1つの実現形態としては、コンテンツ受信機あるいはコンテンツ記録再生機内で、異なるRMP仕様をインストールした複数のハードウェアRMPモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアRMPモジュールに切り替えて利用することが挙げられる。

【0074】また、他の実現形態として、ソフトウェア・モジュールとしてRMPモジュールを構成し、各受信コンテンツ毎に適合するソフトウェア・モジュールを所定のサーバからダウンロードするか、あるいは権利処理メタデータを解析して、所望のソフトウェア・モジュールをコンテンツ受信機側で自動生成することが挙げられる。

【0075】図2には、異なるRMP仕様をインストールした複数のハードウェアRMPモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアRMPモジュールに切り替えて利用する形式のコンテンツ受信機10の構成を模式的に図解している。

【0076】図面に示すコンテンツ受信機10は、フロント・エンド部11と、CAS処理部12と、コンテンツ蓄積用のハード・ディスク装置13A並びに13Bと、RMP識別部14と、それぞれ異なるRMP仕様記述に基づく2つ(複数)のRMPモジュール1並びにRMPモジュール2とで構成される。

【0077】フロント・エンド部11は、所定チャンネルの放送波のチューニングすなわち選局処理と、受信デ-

ータの復調処理を行う。

【0078】CAS処理部12は、コンテンツ配信事業者との間で交わされたCAS(Conditional Access System(限定受信))に関する契約に基づき、放送コンテンツに適用されたスクランブル処理の解除(デスクランブル)を行う。日本国内のデジタル放送では、BS、CSともに共通の「MULTI2」と呼ばれるスクランブル方式を採用する。但し、CAS処理自体は本発明の要旨に関連しないので、ここではこれ以上説明しない。

【0079】ハード・ディスク装置13A及び13Bは、受信コンテンツの蓄積に使用される。より具体的には、一方のハード・ディスク装置13AはRMPモジュールによる権利処理前の状態のコンテンツの蓄積に使用され、他方のハード・ディスク装置13Bは権利処理後の状態のコンテンツの蓄積に使用される。但し、ハード・ディスク装置13A及び13Bは、物理的に互いに独立した装置である必要はなく、例えば、単一のハード・ディスク上に割り当てられた別個の記憶領域(パーティション)であってもよい。

【0080】本実施例では、権利処理メタデータの一部として記述されるRMPには、その方式を識別するための固有の識別情報(RMP ID)が割り振られている。RMP識別部14は、ハード・ディスク装置13Aから権利処理メタデータを読み出して、RMP IDを識別して、2つ(複数)のRMPモジュール1並びにRMPモジュール2のうち識別されたRMP IDに対応する方を動作可能にする。

【0081】RMPモジュール1並びにRMPモジュール2は、暗号化された映画や音楽などのコンテンツ、並びにコンテンツに付随する権利処理メタデータを処理するための幾つかのインターフェース(前述)を備えている。RMP識別部14により付勢されたRMPモジュール1又はRMPモジュール2は、権利処理メタデータとして記述されたRMP仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置13Bやリムーバブル・メディアへの格納などのコンテンツ処理を行う。

【0082】また、図3には、他の実施形態に係るコンテンツ受信機20の構成を模式的に図解している。コンテンツ受信機20は、異なるRMP仕様をインストールした複数のハードウェアRMPモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアRMPモジュールに切り替えて利用するように構成されている。

【0083】図面に示す例では、コンテンツ受信機20は、フロント・エンド部21と、ハード・ディスク装置23と、RMP識別部24と、各RMPモジュール1及びRMPモジュール2と、デコーダ出力装置25と、同一のデータ・バス26を介して相互接続された構成となっている。

【0084】フロント・エンド部21は、所定チャンネル

の放送波のチューニングすなわち選局処理と、受信データの復調処理を行う。但し、図示しないが、放送波を介さない代わりに、インターネットなどの広域ネットワーク経由で所定のサービス・プロバイダからコンテンツを受信する場合においては、フロント・エンド部21は、ネットワーク・インターフェース・カードで実現することができる。

【0085】ハード・ディスク装置23は、RMPモジュールによる権利処理前の状態のコンテンツを蓄積したり、権利処理後の状態のコンテンツを蓄積するために使用される。

【0086】権利処理メタデータとして記述されるRMP IDには、その方式を識別するための固有の識別情報RMP IDが割り振られている。RMP識別部24は、ハード・ディスク装置23から権利処理メタデータを読み出して、RMP IDを識別して、2つ（複数）のRMPモジュール1並びにRMPモジュール2のうち識別されたRMP IDに対応するものを動作可能にする。

【0087】RMPモジュール1並びにRMPモジュール2は、暗号化された映画や音楽などのコンテンツ、並びにコンテンツに付随する権利処理メタデータを処理するための幾つかのインターフェース（前述）を備えている。RMP識別部24により付勢されたRMPモジュール1又はRMPモジュール2は、権利処理メタデータとして記述されたRMP IDを識別し、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置23やリムーバブル・メディアへの格納などのコンテンツ処理を行う。なお、CAS方式を採用するコンテンツ配信事業者からコンテンツを受信する場合には、対応する暗号解読・デスクランブル処理を行うCASモジュールをRMPモジュール上に搭載するようにしてもよい。

【0088】デコーダ出力装置25は、権利処理後の再生コンテンツのデコード処理並びに図解を行う。例えば、AVコンテンツであれば、デコーダ出力装置25は、コンテンツを圧縮映像データと圧縮音声データに分離処理する。そして、MPEG2などによる圧縮映像データを伸張処理して、元のビデオ信号を再生するとともに、圧縮音声データに関しては、PCM（Pulse Code Modulation）デコードした後に付加音と合成して再生音声信号とする。

【0089】また、図4には、他の実施形態に係るコンテンツ受信機30の構成を模式的に図解している。コンテンツ受信機30は、ソフトウェア・モジュールとしてRMPモジュールを構成し、各受信コンテンツ毎に適合するソフトウェア・モジュールを所定のサーバからダウンロードするようになっている。

【0090】図面に示すように、コンテンツ受信機30は、フロント・エンド部31と、CPU（Central Processing Unit）32と、ハード・ディスク装置33A及

び33Bと、RMP識別部34と、作業メモリ35と、デコーダ出力装置36と、ネットワーク・インターフェース37が、システム・バス38を介して相互接続された構成となっている。

【0091】フロント・エンド部31は、所定チャネルの放送波のチューニングすなわち選局処理と、受信データの復調処理を行う。

【0092】ネットワーク・インターフェース37は、TCP/IP（Transmission Control Protocol/Internet Protocol）などの所定の通信プロトコルに従ってコンテンツ受信機37をインターネットなどの広域ネットワークに接続するための装置である。インターネット上には無数のホスト端末が接続されている。ホスト端末の一部は、映画や音楽などのコンテンツを配信する情報配信サーバであり、他の一部はソフトウェアRMPモジュールを配信するサーバである。なお、放送経路でコンテンツを受信する代わりに、インターネットなどの広域ネットワーク経由で所定のサービス・プロバイダからコンテンツを受信する場合においては、フロント・エンド部31は、ネットワーク・インターフェース37によって実現することができる。

【0093】CPU32は、オペレーティング・システム（OS）の制御下で、コンテンツ受信機30内の動作を統括的に制御する中央コントローラであり、作業メモリ35を用いて各種のプログラム・コードを実行する。

【0094】ハード・ディスク装置33Aは、RMPモジュールによる権利処理前の状態でのコンテンツの蓄積、並びに、権利処理後の状態のコンテンツの蓄積に使用される。また、ハード・ディスク装置33Bは、以前使用した（あるいはあらかじめダウンロードしておいた）ソフトウェアRMPモジュールの蓄積に利用される。ハード・ディスク装置33Aと33Bは、それぞれ独立した装置ユニットである必要はなく、例えば単一のハード・ディスク装置上で区切られた記憶領域（例えばパーティション）であってもよい。

【0095】権利処理メタデータとして記述されるRMP IDには、その方式を識別するための固有の識別情報RMP IDが割り振られている。RMP識別部34は、ハード・ディスク装置33から権利処理メタデータを読み出して、RMP IDを識別して、該当するソフトウェアRMPモジュールが作業メモリ35上にロードされて現在使用中か否かを検出する。RMP識別部34は、ハードウェア・コンポーネントとしてではなく、CPU32が実行するプログラム・コードとして実装することもできる。

【0096】作業メモリ35上のソフトウェアRMPモジュールが、これから再生するコンテンツに関するRMP IDにヒットしない場合には、該当するソフトウェアRMPモジュールをローカル・ディスク33B上で探索し、見つかった場合にはこれを作業メモリ35上のも

のと置き換える。ローカル・ディスク33B上で該当するソフトウェアRMPモジュールを発見することができなかった場合には、さらに、ネットワーク・インターフェース37経由でネットワーク上のサーバにアクセスして、所望のソフトウェアRMPモジュールを探索することができる。

【0097】CPU32は、作業メモリ35上にロードされたソフトウェアRMPモジュールを実行することにより、権利処理メタデータとして記述されたRMP仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置33Aやリムーバブル・メディアへの格納などのコンテンツ処理を行うことができる。なお、CAS方式を採用するコンテンツ配信事業者からコンテンツを受信する場合には、対応する暗号解読・デスクランブル処理を行うCASモジュールを同様に作業メモリ35上にロードすればよい。

【0098】デコーダ出力装置36は、権利処理後の再生コンテンツのデコーダ処理並びに外部出力を行う。例えば、AVコンテンツであれば、デコーダ出力装置36は、コンテンツを圧縮映像データと圧縮音声データに分離処理する。そして、MPEG2などによる圧縮映像データを伸張処理して元のビデオ信号を再生するとともに、圧縮音声データに関してはPCM (Pulse Code Modulation) デコードした後に付加音と合成して再生音声信号とする。

【0099】図5には、コンテンツ受信機30にソフトウェアRMPモジュールをダウンロードするための処理手順をフローチャートの形式で示している。以下、このフローチャートに従って、ソフトウェア・モジュールのダウンロード処理について説明する。

【0100】ハード・ディスク装置33Aに蓄積しておいたコンテンツの再生を開始する際、対応する権利処理メタデータを同様にハード・ディスク装置33Aから読み出して、RMPモジュールのRMP IDを取得する(ステップS1)。そして、このRMP IDが現在作業メモリ35にロードされているRMPモジュールのそれと一致するかどうかをチェックする(ステップS2)。

【0101】RMP IDがヒットする、すなわち、これから再生するコンテンツのRMPモジュールが既に作業メモリ35上にロードされている場合には、続いて管理センタと接続確立して、RMP仕様記述に基づいてコンテンツ購入に関する課金処理を行った後(ステップS3)、コンテンツ再生を行い(ステップS4)、本処理ルーチン全体を終了する。

【0102】他方、RMP IDがヒットしなかった場合には、RMP入手先情報を取得して(ステップS5)、RMP入手先となるサーバに接続して(ステップS6)、該当するソフトウェアRMPモジュールをこのサーバからダウンロードする(ステップS7)。もし

て、ダウンロードしたソフトウェアRMPモジュールをコンテンツ受信機30にインストール(例えば、作業メモリ35上にロード)する(ステップS8)。

【0103】RMP入手先情報は、例えば権利処理メタデータ内にURL (Uniform Resource Locator) 形式で記述されている。このような場合、コンテンツ受信機30は、ネットワーク・インターフェース37経由でインターネットのようなTCP/IPネットワーク経由でURLで指示されたサーバに対し資源アクセスして、該当するRMPモジュールをHTTP (Hyper Text Transfer Protocol) 又はFTP (File Transfer Protocol) などの転送プロトコルに従ってダウンロードすることができる。

【0104】新規のソフトウェアRMPモジュールをインストールした結果、コンテンツ受信機30において、権利処理メタデータとして記述されたRMP仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置33Aやリムーバブル・メディアへの格納などのコンテンツ処理を行うことができるようになる。

【0105】続いて、管理センタと接続確立して、RMP仕様記述に基づいてコンテンツ購入に関する課金処理を行った後(ステップS3)、コンテンツ再生を行い(ステップS4)、本処理ルーチン全体を終了する。

【0106】ソフトウェア・モジュールとしてRMPモジュールを構成する変形例として、CPU32(あるいは他の演算処理ユニット)が権利処理メタデータ内のRMP仕様記述を解析して、所望のソフトウェアRMPモジュールをコンテンツ受信機30内部で自動生成するようにしてもよい。

【0107】図6には、ソフトウェアRMPモジュールをコンテンツ受信機30内部で自動生成するための処理手順をフローチャートの形式で図解している。以下、このフローチャートに従って、ソフトウェアRMPモジュールの自動生成処理について説明する。

【0108】ハード・ディスク装置33Aに蓄積しておいたコンテンツの再生を開始する際、対応する権利処理メタデータを同様にハード・ディスク装置33Aから読み出して、RMPモジュールのRMP IDを取得する(ステップS11)。そして、このRMP IDが現在作業メモリ35にロードされているRMPモジュールのそれと一致するかどうかをチェックする(ステップS12)。

【0109】RMP IDがヒットする、すなわち、これから再生するコンテンツのRMPモジュールが既に作業メモリ35上にロードされている場合には、続いて管理センタと接続確立して、RMP仕様記述に基づいてコンテンツ購入に関する課金処理を行った後(ステップS13)、コンテンツ再生を行い(ステップS14)、本処理ルーチン全体を終了する。

【0110】他方、RMP IDがヒットしなかった場合には、RMP仕様記述に関する情報を権利処理メタデータから取得する(ステップS15)。次いで、コンテンツ受信機30上のコンピューテーション・パワー(例えば、CPU32が持つ計算能力)がRMPモジュールを生成するに足りるか否かをチェックする(ステップS16)。

【0111】コンピューテーション・パワー不足の場合には、コンテンツの再生が不可である旨のメッセージを表示した後(ステップS19)、本処理ルーチンを異常終了する。

【0112】他方、コンピューテーション・パワーが充分であった場合には、さらに、RMP仕様記述を解読して(ステップS17)、作業メモリ35上でRMPを設定する(ステップS18)。新規にRMPを設定した結果、コンテンツ受信機30上において、権利処理メタデータとして記述されたRMP仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置33Aやリムーバブル・メディアへの格納などのコンテンツ処理を行うことができるようになる。

【0113】続いて、管理センタと接続確立して、RMP仕様記述に基づいてコンテンツ購入に関する課金処理を行った後(ステップS13)、コンテンツ再生を行い(ステップS14)、本処理ルーチン全体を終了する。

【0114】なお、ハードウェア・モジュールとしてRMPモジュールを構成した場合、ソフトウェアによりモジュールを実装する場合に比し、簡単に他のRMPモジュールに置き換えることはできない。このような場合、サーバ側において、受信機に対応したRMPに置き換えるような仕組みを提供してもよい。例えば、コンテンツ受信機側は、コンテンツのIDでサーバに問い合わせ、コンテンツの変換を依頼する。権利処理条件が整っていれば、所定のRMPに変換することができ、変換後のコンテンツ(あるいは、あらかじめ同じコンテンツが用意されていることでもよい)を依頼元のコンテンツ受信機にダウンロードすることで、希望するコンテンツの復号化・再生を実現することができる。

【0115】次いで、コンテンツ・プロバイダが衛星放送を利用してコンテンツ配信を行うコンテンツ配信システムに対して本発明を適用した場合の実施例について説明する。

【0116】図7には、コンテンツ配信システム100の概略的構成を図解している。同図に示すコンテンツ配信システム100は、コンテンツを制作・提供する番組制作会社又は委託放送事業者からなるコンテンツ・プロバイダ200と、制作・提供されたコンテンツを衛星放送によって配信する衛星放送受託放送事業者(以下、単に「放送局」とする)300と、各一般家庭などに設置されたコンテンツ配信対応衛星放送受信機(以下、単

に「コンテンツ受信機」とする)400とで構成される。コンテンツ受信機400は、一般に、映像及び音声出力用のテレビジョン(TV)450と接続されている。

【0117】コンテンツ・プロバイダ200と放送局300の間では、コンテンツ制作・提供に関する委託契約が交わされており、コンテンツ・プロバイダ200が制作(あるいは外部のコンテンツ・プロバイダから取得した)コンテンツは放送局300に提供される。放送局300は、コンテンツを暗号化して、これを衛星放送波にのせて各家庭内のコンテンツ受信機400に向けて配信する。

【0118】コンテンツ・プロバイダ200は、コンテンツ制作事業者としての番組制作会社201とは独立した、コンテンツ課金を管理する外部の管理センタ202のような決済専門の機関と契約していてもよい。このような場合、コンテンツ・プロバイダ200はコンテンツを暗号化する鍵の管理を管理センタ202に委ね、管理センタ202はコンテンツ販売情報を渡す。

【0119】管理センタ201は、さらに外部の認証局250や他の決済機関と連動していてもよい。また、管理センタ202は、個々のコンテンツ受信機400との間で定期的あるいは不定期的に接続され、コンテンツ受信機400に対して暗号化コンテンツを利用可能にするための鍵情報を配布する。コンテンツ受信機400は、配布された鍵情報を用い、RMP仕様記述に基づいて、放送衛星301経由で受信した暗号化コンテンツを解読して利用に供する。また、コンテンツ受信機400は、ハード・ディスク装置のような大容量外部記憶装置を内蔵しており、受信したコンテンツを蓄積することができる。

【0120】また、コンテンツ受信機400から管理センタ201に対しては、コンテンツの再生ログなど課金情報が送られてくる。コンテンツ受信機400側のユーザは、例えば、コンテンツ使用回数相当の課金額を管理センタに対して月々決済すればよい。決済方法は、現金納付、所定の金融機関への振り込み、プリペイド・カードによる予約、クレジット・カードによる信用決済、デビット・カードによる即時決済、電子マネーの利用などいずれでもよい。

【0121】図8には、コンテンツ制作並びに配信を行う放送局300における構成を模式的に図解している。以下、図8を参照しながら、コンテンツ配信時における暗号化などの仕組みについて説明する。

【0122】コンテンツ暗号化部311は、コンテンツ・プロバイダから提供された映像や音楽などのコンテンツを、コンテンツ鍵(コンテンツ・キー)Kcを用いて暗号化する。但し、コンテンツ・プロバイダから提供されたコンテンツは、コンテンツ・プロバイダにおいて策定されたRMP仕様記述に則った暗号化その他の権利処

理が適用されているものとする。

【0123】コンテンツ鍵暗号化部312は、配信鍵（ディストリビューション・キー）K0を用いてコンテンツ鍵Kcを暗号化する。

【0124】マルチプレクス313は、コンテンツ暗号化部311から入力する暗号化コンテンツと、コンテンツ鍵暗号化部312から入力する暗号化コンテンツ鍵を多重化して、トランスポート・ストリームTS（Transport Stream）を生成する。トランスポート・ストリームは、暗号化コンテンツにメタデータや、暗号化コンテンツ鍵が付加されたデータ・ストリームである。

【0125】CASスクランブラ314は、コンテンツ受信機400において限定受信させるべく、トランスポート・ストリームをスクランブルするや複製処理する。CASにおける契約情報やスクランブル鍵などは、例えば図示しない暗号化装置により暗号化され、放送波にのせてコンテンツ受信機400側に送信することができる。

【0126】図9には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機の一例400Aの構成を模式的に示している。図9に示すコンテンツ受信機400Aは、受信したコンテンツをハード・ディスクなどの所定のローカル記憶装置に一旦蓄積した後でコンテンツの購入を決定するタイプである。以下、図9を参照しながらコンテンツ受信機400Aについて説明する。

【0127】CASデスクランブラ411は、図示しないフロント・エンドにより受信されたデータを、放送局300側から取得したスクランブル鍵を用いてデスクランブルして、トランスポート・ストリームを再現する。

【0128】デマルチプレクス412は、トランスポート・ストリームを、暗号化コンテンツと暗号化コンテンツ鍵とに分離する。分離後、これらは権利処理前の状態のままハード・ディスク装置413Aに一旦蓄積される。

【0129】RMPモジュール420は、ハードウェア・モジュールあるいはソフトウェア・モジュールいずれの形態で実装されていてもよい。ハード・ディスク装置413Aに蓄積したコンテンツを購入する際、まず、対応する権利処理メタデータが読み出され、その中からRMP識別情報（RMP ID）が検出され、適当なRMPモジュールが選択的に動作しているものとする。

【0130】RMPモジュール420は、コンテンツ購入に関する契約を交わした（あるいはユーザ・アカウントを取得している）管理センタ202と接続して、コンテンツの配信鍵K0を購入する。コンテンツ鍵復号化部421は、権利処理メタデータから暗号化コンテンツ鍵を取り出して、これを配信鍵K0で復号化してコンテンツ鍵Kcを得る。後続のコンテンツ鍵再暗号化部422は、RMPモジュール420で規定されているコンテン

ツ蓄積用の鍵（ストレージ・キー）Ksを用いてコンテンツ鍵Kcを再暗号化する。

【0131】購入した暗号化コンテンツを、再暗号化されたコンテンツ鍵とともに、ハード・ディスク装置413Aからハード・ディスク装置413Bに移動する。但し、ハード・ディスク装置413Aと413Bは、物理的に独立した装置ユニットである必要はなく、同一のハード・ディスク内で権利処理前（購入前）と権利処理後（購入後）として記憶領域（例えば、パーティション）を区切られたものであってもよい。

【0132】RMPモジュール420は、購入コンテンツのための配信鍵K0の購入や、購入コンテンツの移動などの処理ログを、課金データとして蓄積しておく。そして、定期的あるいは不定期的に管理センタ202に接続して、課金データを転送する。

【0133】また、図10には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機400Bの構成を模式的に示している。図9に示すコンテンツ受信機400Bは、受信したコンテンツを一旦ハード・ディスクなどのローカル記憶装置に蓄積した後、コンテンツを再生を行うタイプである。コンテンツ受信機400Bは、上述したコンテンツ受信機400Aにより購入・蓄積された暗号化コンテンツの再生装置としても機能する。以下、図9を参照しながらコンテンツ受信機400Bについて説明する。

【0134】ハード・ディスク装置433内には、RMPモジュール440で規定されたコンテンツ鍵Kcを用いて暗号化されたコンテンツと、RMPモジュール440で規定されているコンテンツ蓄積用の鍵（ストレージ・キー）Ksで暗号化された暗号化コンテンツ鍵が格納されている。

【0135】コンテンツ購入時には、コンテンツ鍵復号化部441は、ハード・ディスク装置433から該当する暗号化コンテンツ鍵を読み出して、これを規定された格納鍵Ksを用いて復号化して、コンテンツ鍵Kcを得る。

【0136】コンテンツ復号化部442は、購入したい暗号化コンテンツをハード・ディスク装置433から読み出して、これを復号化されたコンテンツ鍵Kcを用いて復号化し、元の映像又は音楽などのコンテンツを再現する。

【0137】APS処理部443は、ビデオ信号などのアナログ出力信号に対して、マクロビジョンやCGMS-Aなどのコンテンツ保護処理を適用した後、再生コンテンツとしてテレビジョン（図示しない）などの出力装置に送出する。

【0138】図9及び図10に示すようなコンテンツ受信機400Aによれば、コンテンツ・プロバイダは、CASとは独立した暗号化システムによりコンテンツを配信することができる。すなわち、CASに依存しないコ

コンテンツ配信システムなので、異なるCAS（異なる放送事業者）にまたがった共通のプラットフォーム上でコンテンツ購入に対する課金処理を行うことができる。この場合、CASは、単なるコンテンツの流通経路に過ぎない。コンテンツは暗号化されたままの状態ハード・ディスク装置のようなローカル記憶装置に蓄積される。購入時に、コンテンツを解くための鍵がコンテンツ鍵Kから格納鍵Ksにかけ変えられるので、その後は同じコンテンツ受信機400A上でいつでも再生することができる。また、コンテンツ購入処理時に課金するためのログが作成され、定期的あるいは不定期的に管理センタ202に送信されるので、コンテンツ利用者に対して確実に課金・決済を行うことができる。

【0139】図11には、図9に示したようなコンテンツ受信機400Aにおいて、受信コンテンツをハード・ディスク装置413Aに蓄積するための処理手順の一例をフローチャートの形式で示している。受信コンテンツは、基本的には、権利処理前のまま蓄積される。以下、このフローチャートに従って、コンテンツの蓄積処理について説明する。

【0140】まず、コンテンツ受信機400Aのユーザにより予約したい番組が決まっているか否か（すなわち予約設定されているか否か）をチェックする（ステップS21）。

【0141】予約したい番組が既に決められている場合には、例えばデジタル放送であればデータ放送用データの中からEPG（Electric Program Guide：電子番組表）を取り出し、EPGを基に予約すべき番組を選択する（ステップS22）。そして、予約すべき時刻（放映時間帯）並びにチャンネルなどを設定する（ステップS23）。

【0142】次いで、ユーザからのプリファレンス入力（ステップS24）を基に、プリファレンスにあった番組を所定の検索エンジンが自動選択する（ステップS25）。そして、予約すべき時刻（時間帯）並びにチャンネルなどを設定する（ステップS26）。

【0143】予約開始時刻に到達した、あるいは選択された番組IDが受信されたことに応答して、ハード・ディスク装置への受信コンテンツの自動蓄積を行う（ステップS27）。

【0144】また、図12には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機400Cの構成を模式的に示している。図10に示すコンテンツ受信機400Cは、ICカード化された衛星放送用のCASモジュール、すなわちBS-CAS ICカードを内蔵しており、受信したコンテンツを一旦ハード・ディスク装置に蓄積した後、CASシステムに基づいて衛星放送を限定受信して視聴するタイプである。以下、同図を参照しながら、コンテンツ受信機400Cについて説明する。

【0145】図示しないフロント・エンドにより受信されたデータ・コンテンツは、権利処理前であつたCASによりスクランブル処理された状態のまま、ハード・ディスク装置453のような大容量記憶装置に一時蓄積される。

【0146】受信コンテンツの権利処理はRMPモジュール460により行われる。RMPモジュール460は、ハードウェア・モジュールあるいはソフトウェア・モジュールいずれの形態で実装されていてもよい。ハード・ディスク装置453に蓄積したコンテンツを購入する際、対応する権利処理メタデータが読み出され、RMP識別情報（RMP ID）が検出され、適当なRMPモジュールが選択的に動作しているものとする。図示の例では、ICカードとして提供されるCASモジュールはRMPモジュール460の一部を構成する。

【0147】蓄積されたコンテンツを再生する際、該当する権利処理メタデータをハード・ディスク装置453から読み出す。

【0148】権利処理メタデータ中には、ECM（Entitlement Control Message）とEMM（Entitlement Management Message）が含まれている。ECMは、CASスクランブルを解除するためのスクランブル鍵Kscを暗号化したものである。また、EMMは、ECMを解くためのワーク鍵を、契約期間などの契約内容やメッセージとともに暗号化したものである。

【0149】復号部462は、BS-CAS ICカードに記録されているマスター鍵Kmを用いてEMMを解読してワーク鍵と契約情報を得る。次いで、復号部461は、ワーク鍵を用いてECMを解読して、スクランブル鍵Kscを得る。

【0150】判定部464は、復号部462において得られた契約情報に基づき、コンテンツ受信機400Cの正当性を検証する。正当と判定した場合、スクランブル鍵Kscを復号部465に供給する。

【0151】ハード・ディスク装置453に蓄積された受信コンテンツは、CASに基づき、Multi 2などの方式によりスクランブル処理されている。復号部465は、再生すなわち視聴したいコンテンツをハード・ディスク装置453から取り出して、スクランブル鍵Kscを用いてデスクランブル処理する。

【0152】APS処理部466は、ビデオ信号などのアナログ出力信号に対して、マクロビジョンやCGMS-Aなどのコンテンツ保護処理を適用した後、再生コンテンツとしてテレビジョン（図示しない）などの出力装置に送出する。

【0153】一方、復号部462において得られた契約情報は、PPVデータ格納部463に蓄積される。RMPモジュール460は、定期的あるいは不定期的に管理センタ202に接続して、PPVデータを転送する。管理センタ202は、PPVデータを基に、コンテンツ利

用者に対する課金処理を行うことができる。

【0154】図12に示すコンテンツ受信機400Dの構成によれば、CASをそのまま蓄積コンテンツの課金に利用することができる。CASに従って暗号化されたコンテンツは、暗号化されたままハード・ディスク装置に蓄積される。CASで用いられるマスター鍵KmによりECM並びにECMを解いて、蓄積コンテンツを解くことができる。その際、暗号を解いたことを課金ログとして記録する。このような課金ログを定期的あるいは不定期的に管理センタに送信することで、コンテンツ利用者に対して確実に課金を行うことができる。

【0155】また、図13には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機400Dの構成を模式的に示している。同図に示すコンテンツ受信機400Dは、ICカード化された衛星放送用のCASモジュール、すなわちBS-CAS-ICカードを内蔵しており、CASシステムに基づいて衛星放送を限定受信してCASデスクランブルを行った後、再度暗号化してハード・ディスク装置に蓄積するタイプである。以下、同図を参照しながら、コンテンツ受信機400Dについて説明する。

【0156】受信コンテンツの権利処理はRMPモジュール480により行われる。RMPモジュール480は、ハードウェア・モジュールあるいはソフトウェア・モジュールいずれの形態で実装されていてもよい。フロント・エンド部（図示しない）よりコンテンツが受信されたときに、対応する権利処理メタデータが読み出され、RMP識別情報（RMP ID）が検出され、適当なRMPモジュールが選択的に動作しているものとする。同図に示す例では、ICカードとして提供されるCASモジュールや、ハード・ディスク装置に蓄積するコンテンツの保護を行うセキュア・モジュールは、RMPモジュール480の一部を構成する。セキュア・モジュールは、ハード・ディスク装置に蓄積するコンテンツの再暗号化処理、並びに、再生時の暗号解除処理を行う。

【0157】図示しないフロント・エンドにより受信されたデータ・コンテンツのうち、権利処理メタデータは、CASモジュールすなわちBS-CAS-ICカードに入力される。

【0158】権利処理メタデータ中には、ECM（Entitlement Control Message）とECM（Entitlement Management Message）が含まれている。復号部482は、BS-CAS-ICカードに記録されているマスター鍵Kmを用いてECMを解読してワーク鍵と契約情報を得る。次いで、復号部481は、ワーク鍵を用いてECMを解読して、スクランブル鍵Kscを得る。また、復号部482において得られた契約情報は、PPVデータ格納部483に蓄積される。

【0159】判定部484は、復号部482において得られた契約情報に基づき、コンテンツ受信機400Dの

正当性を検証する。正当と判定した場合、スクランブル鍵Kscを復号部485に供給する。

【0160】復号部485は、スクランブル鍵Kscを用いて受信コンテンツをデスクランブル処理して、セキュア・モジュールに出力する。

【0161】セキュア・モジュール内では、暗号化部487が、コンテンツ受信機400Dに固有のコンテンツ蓄積鍵Kstを用いてCASデスクランブル後のコンテンツを再度暗号化して、ハード・ディスク装置473に格納する。

【0162】また、ハード・ディスク装置473に蓄積しておいたコンテンツを再生すなわち視聴する場合には、暗号化コンテンツをハード・ディスク装置473から読み出し、復号部488にてコンテンツ蓄積鍵Kstを用いて復号化する。そして、APS処理部489は、ビデオ信号などのアナログ出力信号に対して、マクロビジョンやCGMS-Aなどのコンテンツ保護処理を適用した後、再生コンテンツとしてテレビジョン（図示しない）などの出力装置に送出する。

【0163】また、セキュア・モジュール内では、CASデスクランブル処理後のコンテンツから権利処理メタデータが取り出され、課金データとして蓄積される。

【0164】RMPモジュール480は、定期的あるいは不定期的に管理センタ202に接続して、CASモジュールにて蓄積されたPPVデータや、セキュア・モジュールに蓄積された課金データを転送する。管理センタ202は、PPVデータを基に、コンテンツ利用者に対する課金処理を行うことができる。

【0165】図13に示すような構成のコンテンツ受信機400Dによれば、CASシステムに従って配信されるコンテンツを再度暗号化して、ハード・ディスク装置に蓄積することができる。再暗号化の際、CASで使用するスクランブル鍵Kscとは異なる鍵構造のコンテンツ蓄積鍵Kstで暗号化する。ハード・ディスク装置に蓄積された暗号化コンテンツを再生する場合には、再生する度に課金ログを生成して、定期的あるいは不定期的に管理センタ202に送信して、コンテンツ利用者に対する課金を行う。CASをRMPモジュールと一体化して構成することもできる。

【0166】[追補] 以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0167】

【発明の効果】以上詳記したように、本発明によれば、映画や音楽などの暗号化された形式で配信される有料コ

コンテンツを特定の利用者が好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【0168】また、本発明によれば、映画や音楽などのコンテンツ制作・提供業者が放送事業者やインターネット・サービス・プロバイダなどの仲介業者を介して配信する暗号化コンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【0169】また、本発明によれば、コンテンツ制作・提供業者自身がコンテンツ利用に関する課金やセキュリティなどを制御可能な形態で配信するコンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【0170】また、本発明によれば、各コンテンツ配信システム毎に策定される複数のRMP (Right Management & Protection) 方式に対応することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【0171】本発明に係るコンテンツ受信装置及びコンテンツ受信方法によれば、1台のコンテンツ受信機を用いて複数の異なるコンテンツ配信方式に対応することができる、配信システム毎の受信機などの機器を用意する必要がなくなる。また、各コンテンツ制作・提供・配信事業者間では、RMP仕様記述などのコンテンツ配信方式の規格化をめぐる争いを沈静化することができる。また、各コンテンツ制作・提供・配信事業者間における配信コンテンツの互換性及び融通性を向上させることができる。また、コンテンツ利用者においては、利便性が高まる。

【図面の簡単な説明】

【図1】RMPモジュールの概念構成を示した図である。

【図2】異なるRMP仕様を実装した複数のハードウェアRMPモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアRMPモジュールに切り替えて利用する形式のコンテンツ受信機の構成を模式的に示した図である。

【図3】異なるRMP仕様を実装した複数のハードウェアRMPモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアRMPモジュールに切り替えて利用する形式のコンテンツ受信機20の他の構成例を模式的に示した図である。

【図4】ソフトウェア・モジュールとしてRMPモジュールを構成し、各受信コンテンツ毎に適合するソフトウェア・モジュールを所定のサーバからダウンロードする形式のコンテンツ受信機30の他の構成例を模式的に示した図である。

【図5】コンテンツ受信機30にRMPモジュールをダウンロードするための処理手順を示したフローチャート

である。

【図6】ソフトウェアRMPモジュールをコンテンツ受信機30内部で自動生成するための処理手順を示したフローチャートである。

【図7】コンテンツ配信システムの概略的構成を示した図である。

【図8】コンテンツ制作並びに配信を行う放送局における構成を模式的に示した図である。

【図9】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の一例400Aの構成を模式的に示した図である。

【図10】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の一例400Bの構成を模式的に示した図である。

【図11】図9に示したコンテンツ受信機400Aにおいて、受信コンテンツをハード・ディスク装置413Aに蓄積するための処理手順の一例を示したフローチャートである。

【図12】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の一例400Cの構成を模式的に示した図である。

【図13】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の一例400Cの構成を模式的に示した図である。

【図14】CASベースのコンテンツ配信システムの概略構成を示した図である。

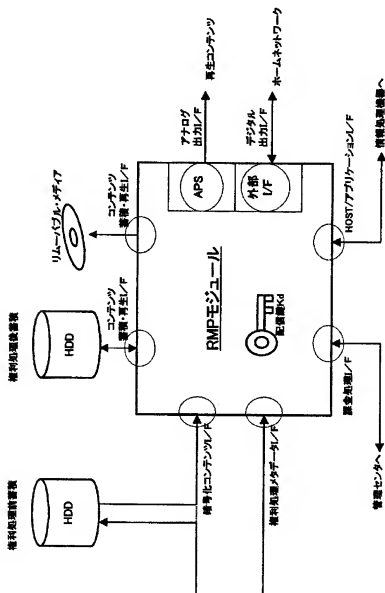
【符号の説明】

10…コンテンツ受信機、11…フロント・エンド部
12…CAS処理部、13A、13B…ハード・ディスク装置
14…RMP識別部
20…コンテンツ受信機、21…フロント・エンド部
23…ハード・ディスク装置、24…RMP識別部
25…デコーダ出力装置
30…コンテンツ受信機、31…フロント・エンド部
32…CPU、33A、33B…ハード・ディスク装置
34…RMP識別部、35…作業メモリ
36…デコーダ出力装置、37…ネットワーク・インターフェース
200…コンテンツ・プロバイダ
201…番組制作会社（委託放送事業者）、202…管理センタ（決済機関）
250…認証局
300…放送局（衛星放送受託放送事業者）、301…放送衛星
311…コンテンツ暗号化部、312…コンテンツ鍵暗号化部
313…マルチプレクサ、314…CASスクランブラ
400…コンテンツ受信機（コンテンツ配信対応衛星放送受信機）

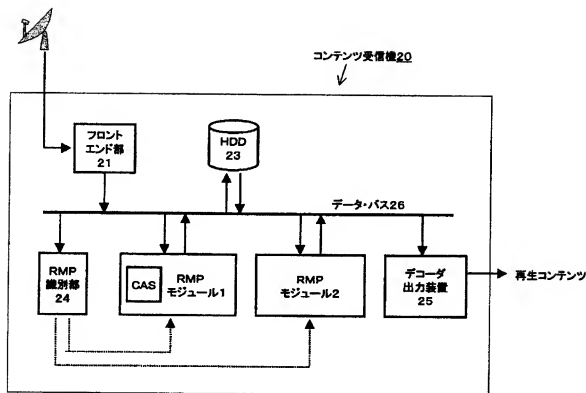
411…CASデスクランブラ、412…デマルチプレクサ
 413A、413B…ハード・ディスク装置
 420…RMPモジュール、421…コンテンツ鍵復号化部
 422…コンテンツ鍵再暗号化部
 433…ハード・ディスク装置、440…RMPモジュール
 441…コンテンツ鍵復号化部、442…コンテンツ復号化部
 443…APS処理部

453…ハード・ディスク装置、460…RMPモジュール
 461…復号部、462…復号部
 463…PPVデータ格納部、464…判定部
 465…復号部、466…APS処理部
 473…ハード・ディスク装置、480…RMPモジュール
 481…復号部、482…復号部
 483…PPVデータ格納部、484…判定部
 485…復号部、487…暗号化部
 488…復号部、489APS処理部

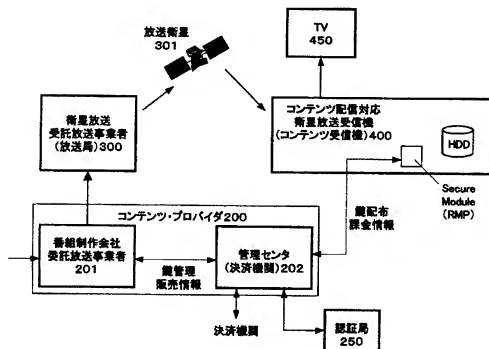
【図1】



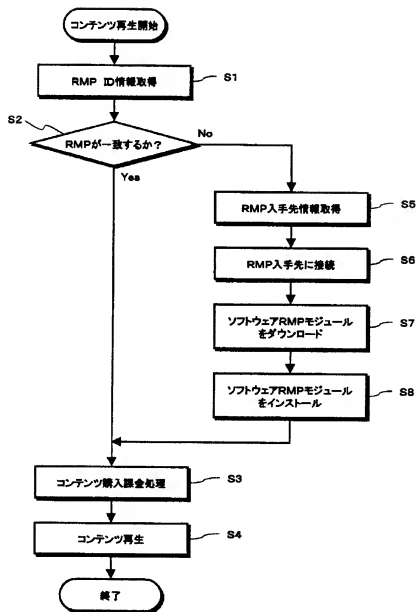
【図3】



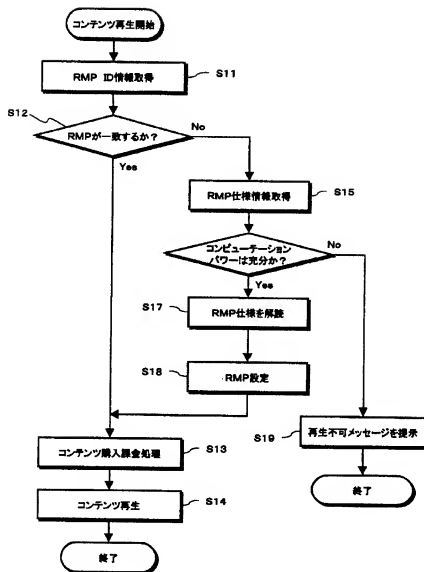
【図7】



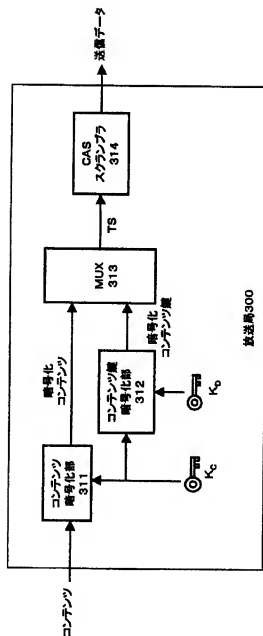
【図5】



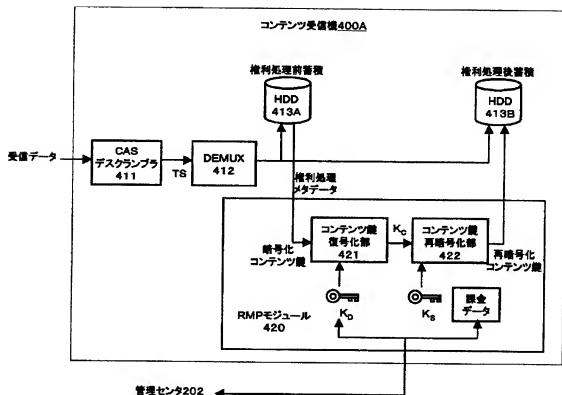
【図6】



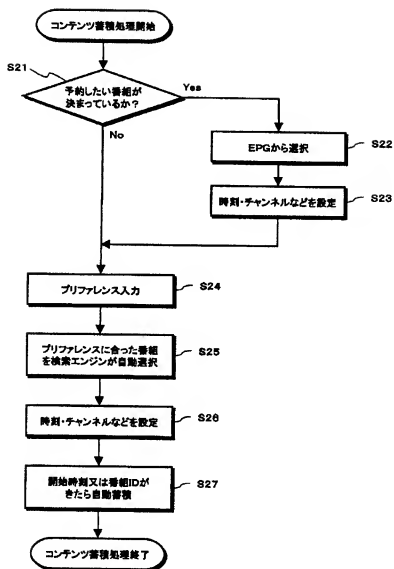
【図8】



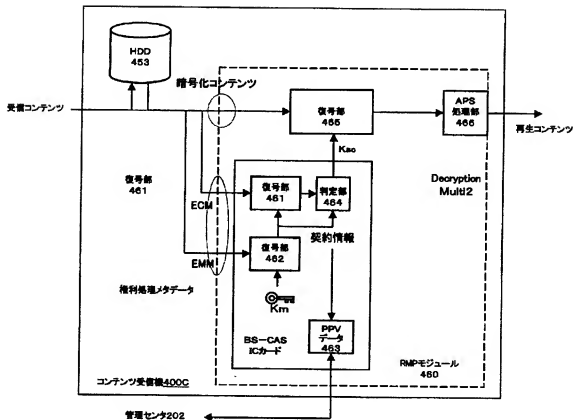
【図9】



【図11】



【図12】



Fターム(参考) 5B085 AA08 AE00 AE29
5C025 BA25 BA27 DA04 DA05
5C064 BA01 BB01 BC03 BC06 BC22
BC25 BD04 BD09 BD14 CA14
5J104 AA01 AA12 AA15 AA16 EA06
EA18 NA02 NA35 NA37 PA05
PA07 PA11